Net-Centric Implementation Framework

Part 1: Overview

Part 2: ASD(NII) Checklist Guidance

Part 3: Migration Guidance

Part 4: Node Guidance

Part 5: Developer Guidance

Part 6: Contracting Guidance for Acquisition

V 2.0

30 April 2007

Net-Centric Enterprise Solutions for Interoperability (NESI) is a collaborative activity of the USN Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I); the USAF Electronic Systems Center (ESC); and the Defense Information Systems Agency (DISA).

Table of Contents

(This page is intentionally blank.)

1 NESI Implementation

NESI Part 4: Node Guidance is the fourth of six parts of the NESI Net-Centric Implementation Document Set. Part 4 provides a set of Perspectives which are a means of organizing and presenting information concerning nodes and encapsulating pertinent guidance and best practices associated with each perspective topic. Note that the best practice statements in this version of Part 4 have a G or BP number (e.g., [G1234] or [BP1234]) which links to the Guidance or Best Practice Details section of Part 4 (as is the case in *NESI Part 5: Developer Guidance*).

Section 1 of Part 4 contains brief NESI background information. For more complete introductory information, see the first part of this document set, *NESI Part 1: Overview*.

1.1 References

(a) DoD Directive 5000.1, *The Defense Acquisition System*, 24 November 2003.

(b) DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, 12 May 2003.

(c) DoD Directive 8100.1, *Global Information Grid (GIG) Overarching Policy*, 21 November 2003.

(d) DoD Directive 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 05 May 2004.

(e) DoD Instruction 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, 30 June 2004.

(f) DoD Directive 5101.7, *DoD Executive Agent for Information Technology Standards*, 21 May 2004.

(g) *DoD Global Information Grid (GIG) Architecture, Version 2.0*, August 2003.

(h) *DoD Architecture Framework (DoDAF), Version 1.0*, 9 February 2004.

(i) *DoD Net-Centric Data Strategy*, DoD Chief Information Officer, 9 May 2003.

(j) CJCSI 3170.01E, *Joint Capabilities Integration and Development System*, 11 May 2005.

(k) CJCSM 3170.01B, *Operation of the Joint Capabilities Integration and Development System*, 11 May 2005.

(l) CJCSI 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems*, 8 March 2006.

(m) *Net-Centric Operations and Warfare Reference Model (NCOW RM)*, Version 1.1 (Draft), 8 November 2004.

(n) *Net-Centric Checklist, V2.1.3*, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 12 May 2004.

(o) *A Modular Open Systems Approach (MOSA) to Acquisition, Version 2.0*, September 2004.

(p) *DoD IT Standards Registry (DISR)*, http://disronline.disa.mil.

(q) *Net-Centric Attributes List*, Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, June 2004.

(r) *Global Information Grid (GIG) Key Interface Profiles (KIPs) Framework (DRAFT)*, Version 0.95, 7 October 2005.

1.2 Overview

Net-Centric Enterprise Solutions for Interoperability (NESI) provides, for all phases of the acquisition of net-centric solutions, actionable guidance that meets DoD Network-Centric Warfare goals. The guidance in NESI is derived from the higher level, more abstract concepts provided in various directives, policies and mandates such as the *Net-Centric Operations and Warfare Reference Model* (*NCOW RM*) and the ASD(NII) *Net-Centric Checklist*, references (m) and (n), respectively. As currently structured, NESI guidance is captured in documents covering architecture, design and implementation; a compliance checklist; and a collaboration environment that includes a repository of guidance statements and code examples.

More specifically, NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology (IT) portion of net-centric solutions for military application. NESI provides specific technical recommendations that a DoD organization can use as references. Stated another way, NESI serves as a reference set of compliant instantiations of these directives.

NESI is derived from a studied examination of enterprise-level needs and, more importantly, from the collective practical experience of recent and on-going program-level implementations. It is based on today's technologies and probable near-term technology developments. It describes the practical experience of system developers within the context of a minimal top-down technical framework. Most, if not all, of the guidance in NESI is in line with commercial best practices in the area of enterprise computing.

NESI applies to all phases of the acquisition process as defined in references (a) and (b) and applies to both new and legacy programs. NESI provides explicit counsel for building in net-centricity from the ground up and for migrating legacy systems to greater degrees of net-centricity.

NESI subsumes a number of references and directives; in particular, the Air Force *C2 Enterprise Technical Reference Architecture (C2ERA)*[1] and the Navy *Reusable Applications Integration and Development Standards (RAPIDS)*.[2] Initial authority for NESI is per the Memorandum of Agreement between Commander, Space and Naval Warfare Systems Command (SPAWAR), Navy PEO C4I & Space and the United States Air Force Electronic Systems Center (ESC), dated 22 December 2003, Subject: Cooperation Agreement for Net-Centric Solutions for Interoperability (NESI). The Defense Information Systems Agency (DISA) formally joined the NESI effort in 2006.

[1] Air Force C2 Enterprise Technical Reference Architecture, v3.0-14, 1 December 2003.

[2] RAPIDS Reusable Application Integration and Development Standards, Navy PEO C4I & Space, December 2003 (DRAFT V1.5).

1.3 Releasability Statement

This document has been cleared for public release by competent authority in accordance with DoD Directive 5230.9 and is granted *Distribution Statement A: Approved for public release; distribution is unlimited*. Obtain electronic copies of this document at http://nesipublic.spawar.navy.mil.

1.4 Vendor Neutrality

The NESI documentation sometimes refers to specific vendors and their products in the context of examples and lists. However, NESI is vendor-neutral. Mentioning a vendor or product is not intended as an endorsement, nor is a lack of mention intended as a lack of endorsement.

Code examples typically use open-source products since NESI is built on the open-source philosophy. NESI accepts inputs from multiple sources so the examples tend to reflect whatever tools the contributor was using or knew best. However, the products described are not necessarily the best choice for every circumstance. Users are encouraged to analyze specific project requirements and choose tools accordingly. There is no need to obtain, or ask contractors to obtain, the open-source tools that appear as examples in this guide. Similarly, any lists of products or vendors are intended only as references or starting points, and not as a list of recommended or mandated options.

1.5 Disclaimer

Every effort has been made to make NESI documentation as complete and accurate as possible. Even with frequent updates, this documentation may not always immediately reflect the latest technology or guidance. Also, references and links to external material are as accurate as possible; however, they are subject to change or may have additional access requirements such as Public Key Infrastructure (PKI), Common Access Card (CAC) use, and user accounts.

1.6 Contributions and Comments

NESI is an open-source project that will involve the entire development community. Anyone is welcome to contribute comments, corrections, or relevant knowledge to the guides via the Change Request tab on the NESI Public site, http://nesipublic.spawar.navy.mil, or via the following email address: nesi@spawar.navy.mil.

1.7 Collaboration Site

The Navy has established a collaboration site to support NESI community interaction. It is located at https://nesi.spawar.navy.mil (user registration required). Use this site for collaborative software development across distributed teams.

2 Nodes

A Node[3] is a collection of Components (i.e., systems, applications, services and other Nodes) which results from the alignment of organizations, technologies, process, or functions. Potential alignment attributes include management, acquisition, mission, technological, sustainment, spatial, or temporal. A Node enables a common strategy for sharing the task of realizing net-centricity and interoperability. As a concept, Nodes may not necessarily be defined in terms of a concrete set of Components or size.

The presumption is that Nodes are actively managed. The shared capabilities necessary to support net-centric interoperability could be provided either by the Node or a system within the Node (i.e., the system is acting as executive agent for the capability).

The discussion of NESI Node guidance is presented in the following perspectives and is largely consistent with the DISA Global Information Grid (GIG) Key Interface Profile (KIP) Framework (Draft v0.9); see reference (r).

- General Responsibilities
- Node Transport
- Node Computing Infrastructure
- Node Application Enterprise Services

Note: A Node might be nested; such cases would likely introduce additional complexities that would require extra management attention and coordination.

The guidance and best practices in these perspectives is meant for those in a position to influence decisions regarding infrastructure and services provided by the Node for shared use by the systems within the Node. With respect to the GIG, the principal question addressed is how should a Node implement the shared infrastructure needed to achieve the DoD vision of broad integration and interoperability across the GIG, on behalf of systems within the Node, and in accordance with DoD policy and direction?

The guidance is applicable to information systems, such as those for command and control or intelligence. It may also be applicable, in part or whole, to other classes of systems or variants, such as embedded or real-time systems, but is aimed principally at systems that have desktop computers, servers, email, Web browsers and such.

Multiple operating environments are considered in the guidance including but not limited to fixed, deployed, mobile air/land/sea Nodes or other instance specific implementations. Occasionally, guidance may be provided for a specific environment or instance of a Node.

Factors such as physical environments and employment concepts directly influence the scope of a Node, and boundaries and can vary widely. As a notional example, consider whether an individual foot soldier should be categorized as a Node. While soldiers are increasingly being outfitted with sensors and computing devices, it is unlikely (in the near term) that an individual

---

[3] The use of the capitalized term *Node* in NESI Part 4, alone or preceded by the term *NESI* (i.e., *NESI Node*) differentiates the specific usage as defined in this section from the more general term *node*.

soldier could host the requisite capabilities needed to ensure compliance with, for instance, the DoD IA Strategy including intrusion detection, firewalls, and such. Rather, a collection of soldiers such as an infantry battalion would be connected to a field command center that provides the requisite infrastructure. Note that this does not preclude an individual soldier from being directly addressable on the Global Information Grid (GIG), able to conduct information exchanges on a global scale. It simply means that requisite infrastructure is unlikely to be isolated to the soldier but rather shared with others. Likewise, nothing precludes the soldier from being a full Node should technology enable the soldier to carry all the requisite infrastructure elements.

2.1 General Responsibilities

In addition to the specific requirements of a Node to support transport, common computing infrastructure, Enterprise Services and Community of Interest (COI) services there are some general responsibilities that a Node must support in order to ensure that the final product can interact with the rest of the Global Information Grid (GIG). The responsibilities include the following:

- Nodes as Stakeholders
- Net-Centric Information Engineering
- Internal Component Environment
- Integration of Legacy Systems
- Orchestration with External Enterprise
- Orchestration of Internal Components

2.1.1 Nodes as Stakeholders

A Node should be formally represented as a stakeholder in the acquisition and evolutionary activities of all the Components it will host. A Node's Component composition will change in the future; maintain and identify all the known Components throughout the lifecycle of the Node. This action is fundamental to the provisioning of a shared infrastructure and the avoidance of functional duplication within the Node.

The necessity of a Node involvement as a stakeholder in its Components may not be obvious; it has a bearing on Global Information Grid (GIG) interoperability. Component independent planning and evolution is likely to result in the external exposure of inconsistencies or, worse, incomplete, inaccurate, or misunderstood data. Consider two systems within the Node that both ingest a particular type of data, but process it at different levels of fidelity, and are independently intending to publish the result to the rest of the GIG. This is an example of when a Node manager would want to work across the systems to ensure that the Node presents its collective capability clearly.

Guidance

- Maintain a comprehensive list of all of the Components that are part of the Node. [G1569]
- Assume an active management role among the Components within the Node. [G1570]

2.1.2 Net-Centric Information Engineering

Of particular concern for Global Information Grid (GIG) interoperability is the information contained in inter-nodal information exchanges. Information exchanges are typically the purview of the systems within the Node, rather than the Node itself, and the details are worked out by a Community of Interest (COI). But the Node infrastructure must be engineered to support information exchanges between various COIs. The COIs can require any number of Components to fulfill the mission, When a Component wishes to make its data available to the enterprise, there are different enterprise design patterns the Component can use. For example, the mechanism selected by a Component to exchange information may be publish-subscribe, broker, or client server. The Node infrastructure must support whichever enterprise design pattern mechanism is selected. Consequently, the Node has a stake in the Component design. Additionally, the Node has a stake in performance specifications provided in the Service Level Agreements (SLA). The Node must support the SLA contract with the Node's infrastructure.

Node management should designate COI representatives to track, advocate, and engineer information exchanges in support of the DoD Net-Centric Data Strategy. According to this strategy, "COI is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange." The principal mechanism for recording COI agreements is the DoD Metadata Registry required by the DoD CIO "DoD Net-Centric Data Management Strategy: Metadata Registration" memo. There are registry implementations on the Non-secure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS).

The DoD Metadata Registry Web site provides a search capability; there is also a SOAP-based interface to the Registry.

Guidance

- Maintain a comprehensive list of all the Communities of Interest (COIs) to which the Components of a Node belong. [G1571]
- Include the Node as a party to any Service Level Agreements (SLAs) signed by any of the Components of the Node. [G1572]
- Define the enterprise design patterns that a Node supports. [G1573]
- Define which enterprise design patterns a Component requires. [G1574]
- Designate Node representatives to relevant Communities of Interest (COIs) in which Components of the Node participate. [G1575]

2.1.3 Internal Component Environment

Nodes should provide an environment to support the development, integration, and testing of net-centric capabilities of their Components. As Nodes themselves and the Components within the Nodes move closer to the implementation of net-centric capabilities, it becomes increasingly important to provide a development, integration, and test environment to support those capabilities. This environment should allow for exercising the Node infrastructure and either

hosting services locally within the Node or providing access to Net-Centric Enterprise Services (NCES). The particulars on how to do this depend on the characteristics of the Node. For example, mobile or deployed Nodes would provide environments substantially different than fixed land-based or permanent Nodes.

At the earliest opportunity within the Node and Component lifecycles, developers should be using the NCES piloted Enterprise Services offered by DISA for development, test, and integration. In the absence of a Node-provided environment, Component developers should use the piloted services directory, through an early adopter agreement, but use of a Node-provided environment at the earliest opportunity is preferable to minimize problems. Potential causes of problems include security parameters, network configuration, and product inconsistencies.

DISA has published an *NCES Pilot Participants Guide* that describes the process for using the piloted services.

Guidance

- Provide an environment to support the development, build, integration, and test of net-centric capabilities. [G1576]
- Maintain an enterprise service schedule for interim and final enterprise capabilities within the Node. [G1577]
- Define a schedule for Components that includes the use of the Enterprise Services defined within the Node's Enterprise Service schedule. [G1578]
- Define which Enterprise Services the Node will host locally when the Node becomes operational. [G1579]
- Define which Enterprise Services will be hosted over the Global Information Grid (GIG) when the Node becomes operational. [G1580]

2.1.4 Integration of Legacy Systems

Nodes might contain systems or applications that are in the Sustainment lifecycle phase. These Components are often referred to as "legacy" systems or applications. Changing the internals of such Components to support net-centricity is impractical and often has little return on investment. Usually, the decisions to brand a system or an application as a "Legacy" system is made at a high level in conjunction with the operational user and acquisition communities. When the legacy functionality needs to be exposed as an interim solution internally to a Node or external to the Node as a proxy it is often accomplished using a service that uses a façade technique. The façade technique is often implemented using a wrapper or an adapter design pattern around the existing legacy system or application.

Guidance

- Expose legacy system or application functionality through the use of a service that uses a façade design pattern. [G1581]

2.1.5 Orchestration of Node and Enterprise Services

The Net-Centric Enterprise Services (NCES) capabilities under definition, development, or in pilot testing are complex and use leading edge technologies. The status, availability and deployment schedule for services should be reflected in an integrated master schedule for the Node that shows planned dependencies of systems within the Node on these services. Given the rate of evolution and leading edge nature of some services, the orchestration of efforts should be detailed, including specific version numbers, workarounds, assumptions, constraints, configuration, and best practices. Note that these practices should be followed for orchestration with both external and Node-provided Enterprise Services.

Guidance

- Maintain an enterprise service schedule for interim and final enterprise capabilities within the Node. [G1577]
- Define a schedule for Components that includes the use of the Enterprise Services defined within the Node's Enterprise Service schedule. [G1578]
- In Nodal Enterprise Services schedules, include version numbers of standard Enterprise Services interfaces being implemented. [G1582]

2.1.6 Orchestration of Internal Components

The shared infrastructure provided by Nodes, for shared use by its member Components cannot evolve independently of the Components within the Node. Nodes may host a variety of Components and Components may be members of multiple Nodes. Consequently, the development of Components is likely to occur with differing timeframes and rates of evolution. This presents a coordination challenge for the Node managers.

Guidance

- Provide routine Enterprise Services schedule updates to every Component of a Node. [G1583]

2.2 Node Transport

A Node provides a transport infrastructure that is shared among the Components within the Node, implements Global Information Grid (GIG) IA boundary protections, and is Internet Protocol Version 6 (IPv6) capable. In some cases, guidance may seem rudimentary, but history demonstrates that configuration errors for such rudimentary aspects are often the cause of interoperability, integration, and information assurance issues.

The DISA/National Security Agency (NSA) Security Technical Implementation Guidance (STIG) documents are applicable in several places throughout this section. The guidance provided by those documents is not repeated here. The STIG documents are updated frequently as new vulnerabilities are discovered and the current "state of the art" is refined. The applicable STIG documents should be consulted as a fundamental part of design activities, and monitored periodically for updates.

Transport elements provided by a Node are obviously essential in achieving net-centricity but also play a key role in minimizing interoperability issues. The Transport elements are described in the following perspectives:

- Internet Protocol (IP)
- Domain Name System (DNS)
- Routers
- Time Services
- Mobile and Dynamic Networks
- Multicast
- Network Information Assurance Components
- Enterprise Management Services
- Virtual Private Networks (VPN)
- Trusted Guards
- Integration of Non-TCP/IP Transports
- Black Core

***Note*:** The elements described above are in a recommended order of implementation, with the basic enablers described first, for a notional Node. Specific elements and implementation order may vary according to factors such as Node connectivity, scale, mission, and concepts of employment.

Guidance

- Provide a transport infrastructure that is shared among Components within the Node. [G1584]

- Provide a transport infrastructure for the Node that implements Global Information Grid (GIG) Information Assurance (IA) boundary protections. [G1585]

Best Practice

- Consult the applicable Security Technical Implementation Guidance (STIG) documents as a fundamental part of design activities, and monitor the STIGs periodically for updates. [BP1704]

References

- DoD CIO memos:
    - 9 June 2003, "Internet Protocol Version 6 (IPv6)"
    - 29 September 2003, "Internet Protocol Version 6 (Ipv6) Interim Transition Guidance"
    - 28 November 2003, "Internet Protocol Version 6 (IPv6) Transition Plan Coordination and Interim Tasking"
    - Aug. 16 2005 "Internet Protocol Version 6 (Ipv6) Policy Update"
    - 16 August 2005, "DoD Internet Protocol Version 6 (IPv6) Pilot Nominations"

2.2.1 Internet Protocol (IP)

The Assistant Secretary of Defense for Networks and Information Integration, ASD(NII), defines Internet Protocol (IP) as one of nine attributes of net-centricity. It is among the most fundamental of protocols needed for Global Information Grid (GIG) interoperability. There are, however, a number of interoperability challenges emerging as DoD usage of IP networking continues to expand. Two of these areas are the following:

- IPv4 to IPv6 Transition
- Mobile Nodes

2.2.1.1 IPv4 to IPv6 Transition

A 9 June 2003 ASD(NII)/DoD CIO memo, "Internet Protocol Version 6 (IPv6)," is the first in a series of memos (see the References below) addressing DoD transition to IPv6 and establishing IPv6, as the next generation network protocol for DoD with the transition date goal of FY 2008. The DoD IPv6 Transition Office created in DISA is responsible for master transition plan development, acquiring Internet Protocol (IP) addresses, providing necessary infrastructure and technical guidance, and ensuring that unified solutions are used across DoD to minimize cost and interoperability issues. DoD components are tasked with the development of the component transition plans and with providing guidance and governance to programs. Three main Milestone Objectives (MOs)[4] have been outlined for the gradual and controlled transition of the enterprise. Currently only those systems approved as MO1 pilots are allowed to switch to IPv6 in operational environments.

To enable this transition, as of 1 October 2003 all Global Information Grid (GIG) assets being developed, procured, or acquired shall be IPv6 capable (while retaining compatibility with IPv4). The DoD IPv6 Working Group is working on IPv6 implementation issues through formal standards bodies. A high level working definition for "IPv6 capable" is available; the list of the standard IPv6 specifications approved for the use in DoD networks is hosted on DISR[5] website.

Prepare an IPv6 transition plan for the Node infrastructure as well as the transport users within the Node in coordination with the Component and DoD transition plan; the Node IPv6 transition plan is subject to review and approval by the appropriate IPv6 transition authority. Coordination is essential to ensure that the intermediate network infrastructures are IPv6 capable in the planned timeframe, and similarly for other-end network infrastructures for known system interfaces. The Node's IPv6 transition plan should consider applicable DoD Component IPv6 transition plans, IPv6 working group products, and include interoperability testing in the plan. The net-centric concepts of loose coupling and discoverable services may be impacted by the transition to IPv6 if services begin depending on IPv6-specific features. Services that have been developed to utilize IPv6 features and which may perform differently if accessed via an Internet Protocol Version 4 (IPv4) infrastructure should describe the potential impacts in the Service Registry.

IPv6 transition has an impact on many transport infrastructure components. The IPv6 Transition Plan for a Node should include transition of all impacted network elements including DNS, routing, security, and dynamic address assignment. The DoD IPv6 Network Engineer's

---

[4] March 2005, "The Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan"

[5] DoD IT Standards Registry (DISR), http://disronline.disa.mil

Guidebook (Draft) and the DoD IPv6 Application Engineer's Guidebook (Draft) provide guidance for transition of impacted components.

Guidance

- Provide a transport infrastructure for the Node that is Internet Protocol Version 6 (IPv6) capable in accordance with the appropriate governing transition plan. [G1586]

- Prepare an Internet Protocol Version 6 (IPv6) transition plan for the Node. [G1587]

- Coordinate an Internet Protocol Version 6 (IPv6) transition plan for a Node with the Components that comprise the Node. [G1588]

- Address issues in the appropriate governing IPv6 transition plan as part of the Internet Protocol Version 6 (IPv6) transition plan for a Node. [G1589]

- Prepare IPv6 Working Group products as part of the Internet Protocol Version 6 (IPv6) transition plan for a Node. [G1591]

- Include interoperability testing in the plan as part of the Internet Protocol Version 6 (IPv6) transition plan for a Node. [G1592]

- Include transition of all the impacted elements of the network as part of the Internet Protocol Version 6 (IPv6) Transition Plan for a Node. [G1590]

    - Support both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) simultaneously in the Node's Domain Name System (DNS) service. [G1599]

    - Obtain from DISA any and all Internet Protocol Version 6 (IPv6) addresses used on DoD systems in the Node. [G1600]

Best Practices

- Describe the potential impacts in the Service Registry for services developed to utilize Internet Protocol Version 6 (IPv6) features which may perform differently if accessed via an Internet Protocol Version 4 (IPv4) infrastructure. [BP1660]

- Design DNS infrastructure in accordance with appropriate governing IPv6 Transition Office requirements. [BP1705]

References

- DoD CIO memos:
    - 9 June 2003, "Internet Protocol Version 6 (IPv6)"
    - 29 September 2003, "Internet Protocol Version 6 (Ipv6) Interim Transition Guidance
    - 28 November 2003, "Internet Protocol Version 6 (IPv6) Transition Plan Coordination and Interim Tasking"

- Aug. 16 2005 “Internet Protocol Version 6 (Ipv6) Policy Update”
- 16 August 2005, “DoD Internet Protocol Version 6 (IPv6) Pilot Nominations”

- March 2005, “The Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Plan”

- DoD IT Standards Registry (DISR), http://disronline.disa.mil

2.2.1.2 Mobile Nodes

There have been significant advances in Transmission Control Protocol/Internet Protocol (TCP/IP) connectivity to mobile Nodes, such as airplanes, ships, and battlefield units; however, some significant challenges remain. In particular, it remains unclear to what extent mobile Nodes can directly utilize Enterprise Services, particularly the DISA Core Enterprise Services (CES). The characteristics of the link are likely to be extremely variable, including intermittent connectivity, higher than typical packet loss, low bandwidth, or high latency. Such characteristics are generally problematic for anything but the simplest of Enterprise Services. Components that use these Enterprise Services need to adapt in real-time to the presence or absence of the enterprise service and to the potentially intermittent performance of enterprise services. Consequently, the Component must be able to handle the failover and recover from Enterprise Service errors and gaps.

Managers of mobile Nodes that rely on the Internet Protocol (IP) for inter-Node communication should engage with the DISA Net-Centric Enterprise Services (NCES) program office to explore approaches for mobile use of the CES services. Alternatives might include development of specialized Software Development Kits (SDKs) that implement the required adaptive behavior or use of service proxies within the Node that could failover gracefully.

If high bandwidth, high latency satellite communications are employed, the Node should implement the Internet Engineering Task Force Request for Comments 1323, “TCP Extensions for High Performance” (IETF RFC 1323) which addresses describes adjustment of the TCP sliding window buffer to accommodate large amounts of transmitted data that may be in the pipe and not yet unacknowledged due to the long round-trip times of such links. Failure to make this adjustment could result in poor performance and inability to engage in net-centric interoperability.

Best Practice

- Implement IETF RFC 1323 for high bandwidth, high latency satellite communications. [BP1594]

2.2.2 Domain Name System (DNS)

The Domain Name System (DNS) is a system that stores the relationships of host Internet Protocol (IP) address and their corresponding domain names in the equivalent of a distributed database (used here as a simplistic concept). The most import role of the DNS is to map IP addresses to human friendly domain names and back again. For example, where **`nesi.spawar.navy.mil`** may map to an Internet Protocol Version 4 (IPv4) address of **`128.49.49.225`**, the Internet Protocol Version 6 (IPv6) address might be **`1080::34:0:417A`**. For more information on DNS see RFC 1034. DNS also performs other essential functions, such as

reverse lookups (obtaining host names from Internet Protocol (IP) addresses, which can be important for security) and email configuration (special DNS Mail eXchange (MX) Records indicate the server used to receive email for a host). These capabilities are fundamental to net-centric operations and are essential for other computing, network, and Enterprise Services.

The DNS namespace is hierarchical. At each level in the hierarchy, the namespace can be further divided into sub-namespaces called zones, which are delegated to other authoritative servers, and which can be further divided and delegated to other authoritative servers, and so on.

Each Node should implement DNS to manage hostname/address resolution within the Node, rather than use hard coded IP addresses, and use the DNS Mail eXchange (MX) Record capabilities to configure electronic mail delivery to the Node.

The DNS implementation should reflect the guidance provided in "Domain Name System Security Technical Implementation Guide." The STIG addresses implementation options such as the choice of basic DNS server types (primary, secondary, caching-only), use of a split-DNS design, location of servers in the network and relationship to other network entities, secure administration, security of zone transfers, and initial configuration.

Consider operational performance constraints, such as narrow bandwidth and intermittent connectivity, in the design of the Node's DNS. It may be desirable, for instance, to implement a caching-only DNS server for constrained environments.

Guidance

- Implement Domain Name System (DNS) to manage hostname/address resolution within the Node. [G1595]

- Use Domain Name System (DNS) Mail eXchange (MX) Record capabilities to configure electronic mail delivery to the Node. [G1596]

- Allow dynamic Domain Name System (DNS) updates to the Node's internal DNS service by local Dynamic Host Configuration Protocol (DHCP) server(s). [G1598]

- Support both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) simultaneously in the Node's Domain Name System (DNS) service. [G1599]

- Obtain from DISA, in accordance with appropriate governing policy, any and all Internet Protocol Version 6 (IPv6) addresses used on DoD systems in the Node. [G1600]

Best Practices

- Consider operational performance constraints in the design of the Node's Domain Name System (DNS). [BP1597]

- Follow the guidance provided in the Security Technical Implementation Guide (STIG) for Domain Name System (DNS) implementations. [BP1662]

- Design a Domain Name System (DNS) in coordination with the appropriate governing Internet Protocol Version 6 (IPv6) Transformation Office. [BP1663]

- Design DNS infrastructure in accordance with appropriate governing IPv6 Transition Office requirements. [BP1705]

2.2.3 Routers

Routers not only provide the main connection to the Global Information Grid (GIG), but they also are a first line of computer network defense. These complex devices also provide security filtering, address management, network management, and time synchronization. There is a GIG Router Working Group (GRWG) that is addressing implementation issues.

Components should be able to operate in a heterogeneous environment. The presence of Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) packets and services in a dual stack environment should not cause a degradation of application performance.

Guidance

- Use configurable routers to provide dynamic Internet Protocol (IP) address management using Dynamic Host Configuration Protocol (DHCP). [G1601]
- Use configurable routers to provide static Internet Protocol (IP) address. [G1602]
- Use configurable routers to provide time synchronization services using Network Time Protocol (NTP). [G1604]
- Use configurable routers to provide multicast addressing. [G1605]
- Manage routers remotely from within the Node. [G1606]
- Configure routers according to National Security Agency (NSA) Router Configuration guidance. [G1607]

Best Practices

- Configure routers to provide static addresses as defined by the Network Security Technical Implementation Guide (STIG). [BP1603]
- Configure routers in accordance with the National Security Agency (NSA) Router Security Configuration Guide. [BP1664]
- Configure routers to update the Node's internal DNS service in accordance with the Network Security Technical Implementation Guide (STIG). [BP1665]
- Configure routers in accordance with the Network STIG. [BP1699]
- Configure routers in accordance with the Enclave STIG. [BP1700]

2.2.4 Time Services

Net-centric operations and security depend on date and time synchronization. Many protocols rely upon synchronized time to function properly, particularly security protocols. Mission Component logic and the usefulness of data can also suffer if there is not a common understanding and synchronization of time across the enterprise.

Guidance

- Use configurable routers to provide time synchronization services using Network Time Protocol (NTP). [G1604]

- Obtain the reference time for the Node time service from a globally synchronized time source. [G1608]

- Arrange for a backup time source for the Node time service. [G1609]

2.2.5 Mobile and Dynamic Networks

Nodes can be mobile or deployable as well as fixed. Mobile networks, by their very nature, are untethered and usually reliant upon Radio Frequency (RF) transmissions. While there are many RF and network engineering challenges regarding the implementation of RF, such communications topics are outside the scope of NESI. The challenge to be addressed herein is that of ensuring uninterrupted Global Information Grid (GIG) interoperability as the underlying network changes dynamically.

Note: A goal of mobile or deployable Nodes is that they can plug into different locations in the GIG without loss of interoperability.

2.2.6 Multicast

Multicast addressing currently supports various groups throughout the DoD to provide capabilities such as collaboration and alerting; the use of multicast addressing is growing. Multicast capability is being actively engineered into the Global Information Grid (GIG). Careful planning is still required, however, until multicast becomes ubiquitous across the entire GIG.

Guidance

- Use configurable routers to provide dynamic Internet Protocol (IP) address management using Dynamic Host Configuration Protocol (DHCP). [G1601]

- Configure the Dynamic Host Configuration Protocol (DHCP) services to assign multicast addresses. [G1610]

Best Practice

- Anticipate that multicasting will be required even if not used currently and consider this requirement in the design of the Node's networks including the selection of Components and Configuration. [BP1706]

2.2.7 Network Information Assurance

Implementation of the DoD Information Assurance (IA) Strategic Plan is required to comply with the DoD Net-Ready Key Performance Parameter (NR-KPP). Components that implement IA, however, can be a barrier to interoperability by default; proper implementation is critical. Furthermore, as net-centric applications and services emerge, so too will the need to dynamically configure the IA Components to permit net-centric operations. As an example, access control based on Internet Protocol (IP) address would not work, as the addresses of service users will not be known *a priori* when such services are dynamically discoverable.

The DoD provides requirements and extensive guidance for the implementation of information assurance at the DISA Information Assurance Support Environment (IASE) Web site. In particular, the Network STIG on the IASE Web site provides guidance for the network implementation, particularly the boundary between the Node's internal network and external networks. It identifies several IA systems, capabilities, and configurations as listed below and provides guidance for implementation of each.

Rather than repeating the contents of specific guidance in this document, readers should check the IASE Web site for current Network IA guidance on topics such as the following:

- External Network Intrusion Detection System (IDS), anomaly detection, or prevention device if required by the Computer Network Defense Service Provider (CNDSP)
- Routers Security with Access Control Lists
- Firewall and application level proxies (may be separate device to proxy applications)
- Internal Network Intrusion Detection (NID) system
- DMZ, if applicable for publicly accessible services
- Split Domain Name Service (DNS) architecture
- Secure devices and operating systems (i.e., STIG compliant)
- Ports and protocols

Furthermore, DoD computer network defense (CND) policies "…mandate all owners of DoD information systems and computer networks enter into a service relationship with a CNDS provider."

Best Practice

- Configure Components for Information Assurance (IA) in accordance with the Network STIG. [BP1701]

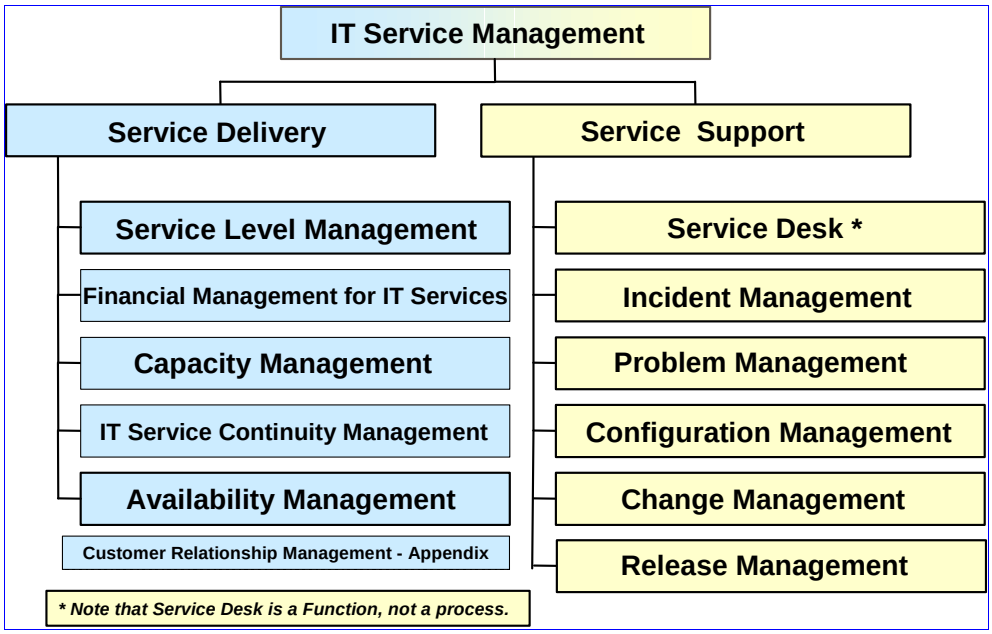
References

- DoD Directive O-8530.1, "Computer Network Defense"
- DoD Instruction O-8530.2, "Support to Computer Network Defense Services (CNDS)"

2.2.8 Enterprise Management Services

Enterprise Management Services (EMS) are fundamental to execution of Service Level Agreements (SLAs), which are inherent in net-centric operations. EMS services are often used internal to a Node using a variety of commercial off-the-shelf (COTS) tools. In a net-centric context, though, EMS must be extended to address inter-nodal service availability and reliability guarantees. Beyond the simpler task of maintaining status information such as link status or service up/down status, EMS must be extended to address complex service arrangement that may

involve multiple, orchestrated services. Additionally, coordinated help-desk and reporting will be needed. Some of these topics are being addressed under the DoD NetOps concept.



2.2.9 Virtual Private Networks (VPN)

Virtual Private Networks (VPNs) create a private "tunnel" within a network by encrypting traffic between specified end points. If a VPN is required at a Node, it should be implemented in accordance with the guidance provided in the Network STIG. Services and information intended to be broadly accessible to other Global Information Grid (GIG) Nodes should not be placed behind a VPN because it will be reachable to only the Nodes that are part of in the VPN.

Best Practices

- Implement a Virtual Private Network (VPN) in accordance with the guidance provided in the Network STIG. [BP1667]

- Do not place services and information intended to be broadly accessible to other Nodes behind a VPN. [BP1702]

2.2.10 Trusted Guards

Trusted guards are accredited to pass information between two networks at different security levels, such as between SECRET General Service (GENSER) and TOP SECRET Sensitive Compartmented Information (SCI) level networks, according to well defined rules and other controls. Guard products only pass defined types of information (e.g., email, images, or formatted messages). A key challenge is how to implement net-centric operations across trusted guards in the presence of CES services. See the Cross-Domain Interoperation perspective (Section 2.4.1.4) for additional information.

Best Practices

- Do not build dedicated Node guard products. [BP1653]

- Do not build dedicated Component guard products. [BP1654]

- Acquire and configure guard products with the help of the Government program offices that acquire such guards. [BP1668]

- Use XML-capable guards in anticipation that net-centric solutions through guards will rely heavily on the passing of XML messages. [BP1669]

2.2.11 Integration of Non-IP Transports

Systems that are not Internet Protocol (IP) networked, such as aircraft data links (Link-16, SADL, etc.), should implement IP gateways to interoperate with the Global Information Grid (GIG) until IP is supported natively. Most such systems already have plans for transition to IP networking, and gateways are an interim measure.

The gateway should be implemented as a service in accordance with *NESI Part 5: Developer Guidance*. This does not mean that the service would be limited to request/reply or other such usage patterns. In fact, for high-frequency data, such as track reporting, a function of the service could be to set up an out-of-band communication with a subscriber.

Guidance

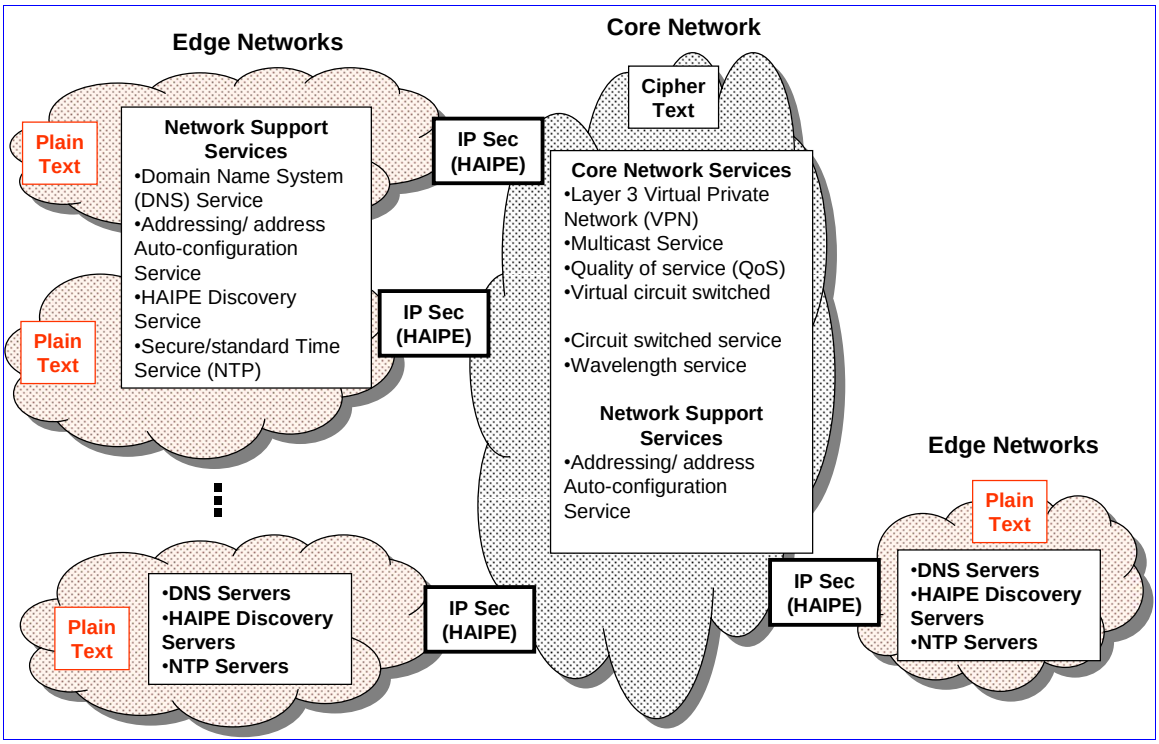
- Implement IP gateways to interoperate with the Global Information Grid (GIG) until IP is supported natively for Components that are not Internet Protocol (IP) networked, such as aircraft data links (Link-16, SADL, etc.). [G1611]

- Implement IP gateways as a service. [G1612]

2.2.12 Black Core

The DoD will be aggregating Internet Protocol (IP) packet traffic from multiple security enclaves onto network segments secured at the network layer in the protocol stacks; these segments are called the *Black Core*, enabled through the use of High Assurance Internet Protocol Encryption (HAIPE) devices. Challenges to the implementation of HAIPE devices and the Black Core include organic support for the following: IP-based quality of service (QoS), dynamic unicast IP routing, support for dynamic multicast IP routing, support for mobility, and support for simultaneous Internet Protocol Version 6 (IPv6) and Internet Protocol Version 4 (IPv4) operation.

The Black Core is a concept fundamental to Global Information Grid (GIG) networking, but it is listed last in this document because there is little actionable guidance that can be provided at this time. Interoperability with the Black Core will require active monitoring by the Node's management and program offices. The basic architecture of the Black Core is shown below. The Node typically provides one or more edge networks as shown in the diagram, along with the services indicated. The edge (Node) networks are sometimes referred to as Plain Text (PT) networks, while the Black Core is the Cipher Text (CT) network.



Best Practices

- Monitor Black Core implementation issues and prepare a plan for local implementation in coordination with system programs fielded within the Node. [BP1670]

- Consider Black Core transition whenever there is a significant Node network design or configuration decision to make in an effort to avoid costly downstream changes caused by Black Core transition. [BP1671]

2.3 Node Computing Infrastructure

Several elements of the computing infrastructure have a significant effect on Global Information Grid (GIG) interoperability. Other elements of the computing infrastructure, such as Host Management, Backup/Restore, and Software/Patch Distribution are outside the scope of NESI because they have little impact on net-centricity or interoperability across GIG Nodes. The following elements have a direct bearing on net-centricity or interoperability:

- Web Client Platform
- Web Application Infrastructure
- Host Information Assurance
- Domain Directories
- Instrumentation and Metrics

2.3.1 Web Client Platform

Web clients (both desktops and servers) should be capable of accessing Java Platform, Enterprise Edition (Java EE) services and .NET services; service developers are free to choose the best technology for their service.

Two key elements of the standard frameworks follow:

- Browser
- CAC Reader

Guidance

- Prepare a Node to host new Component services developed by other Nodes or by the enterprise itself. [G1613]

- Prepare a Node for the possibility of becoming a new Component service within another Node. [G1614]

Best Practices

- Be prepared to integrate fully with the Information Assurance (IA) infrastructure. [BP1672]

- Be prepared to integrate fully with the Enterprise Management Services (EMS) infrastructure. [BP1673]

2.3.1.1 Browser

Web browsers are fundamental to the DoD vision of net-centric information sharing and access to distributed services. Because Global Information Grid (GIG) interoperability partners may not be known *a priori*, Web browsers should support a wide breadth of browser technologies, such as JavaScript, Java applets, and plug-ins.

The browser should be configured in accordance with the Web Server Technical Implementation Guide (STIG), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG.

Guidance

- Use Web browsers that support a wide breadth of browser technologies that can extend the browsers' functionality. [G1615]

Best Practice

- Configure the browser in accordance with the Web Server Security Technical Implementation Guide (STIG), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG. [BP1674]

2.3.1.2 Common Access Card (CAC) Reader

Smart cards provide greatly increased security for multiple applications. The usefulness of a smart card is based on its intrinsic portability and security. A typical smart card has the same dimensions as a standard credit card and appears to be very similar with the exception of a set of gold contacts. When inserted into a reader, these contacts provide power to a microprocessor

located on the smart card; the smart card is thus able to store and process information, in particular cryptographic keys and algorithms for providing digital signatures and for use with other encryption. A major impediment to the widespread use of smart cards has been interoperability. Unfortunately, smart cards are currently not vendor interoperable and therefore must use specific software and smart card readers. This is an issue that is being addressed by the National Institute of Standards and Technology (NIST) Information Technology Laboratory (ITL).

Guidance

- Configure servers with a Common Access Card (CAC) reader. [G1618]
- Configure clients with a Common Access Card (CAC) reader. [G1619]

Reference

- DoD Common Access Card

2.3.2 Web Infrastructure

A Web infrastructure allows software developers to deploy Web-enabled applications, services and other software in a Node. While many Web infrastructures exist, most software will converge on one or two popular platforms or technologies (e.g., Apache, Java Enterprise Edition, .NET, etc.). The Node should provide common shared Web infrastructures for software deployments to minimize unnecessary duplication of these common environments. A common Web infrastructure will also allow Nodes to better provide full integration with local Information Assurance (IA) and Enterprise Management Services (EMS) infrastructures as well as CES and COI services available both internally and externally to the Node.

There are three major elements to Web infrastructure that need to be addressed at the Node:

- Web Portal
- Web Server
- Web Application Containers

Guidance

- Allow all Components that are hosted at a Node to access and use the Node's Web infrastructure. [G1621]

Best Practices

- In the Node's Web infrastructure, support the technologies and standards used by the CES services under development as well as any technologies and standards used for Community of Interest (COI) services. [BP1675]
- Consider using Web proxy servers and load balancers. [BP1677]
- Configure and locate elements of the Node Web infrastructure in accordance with the Web Server STIG. [BP1707]

- Configure and locate elements of the Node Web infrastructure in accordance with the Desktop Applications STIG. [BP1708]

- Configure and locate elements of the Node Web infrastructure in accordance with the Network STIG. [BP1709]

2.3.2.1 Web Portal

A Web portal provides an environment for hosting small Web applications called portlets, and allows for content selection, arrangement and other visual preferences tailored to each user. Though not strictly essential for Global Information Grid (GIG) interoperability, it can reasonably be expected that some GIG net-centric services and applications will provide portal based Web applications that Nodes may want to host locally. To reduce issues of portability, Web portals provided by the Node should support widely accepted standards such as JSR-168 and Web Services for Remote Portlets (WSRP). However, because commercial products also provide non-portable proprietary interfaces, there is a risk that multiple Web portal products may be required or that the portlet would have to be reengineered to work on an existing Node portal. (See the Web Portals perspective in *NESI Part 5: Developer Guidance* for additional information).

Best Practice

- Support appropriate and widely accepted standards for Web portals provided by the Node. [BP1710]

2.3.2.2 Web Server

Web server technology is becoming fundamental in making information visible and accessible to external Global Information Grid (GIG) users. The most significant barrier to interoperation is security. Making information accessible to a community of users as large as the GIG necessitates the implementation of authentication and authorization technology that is sufficient to prove a user's identity and that is scalable, respectively. Web servers should provide DoD Public Key Infrastructure (PKI) based authentication and role based authorization mapped to certificate attributes as described in the applicable STIGs. Eventually, the container should integrate with the Net-Centric Enterprise Services (NCES) Security Service, when available. In the interim, authorization should be based on the Electronic Data Interchange – Personnel Identifier (EDI-PI) contained in the PKI certificate attributes. The use of the EDI-PI as the attribute on which to base authorization decisions is a matter of debate and ongoing engineering, as there are issues about the issuance of EDI-PI to certain user populations, such as coalition users. In the absence of an EDI-PI attribute, other attributes should be used for authorization decisions. (For additional technical level guidance on Web servers, see *NESI Part 5: Developer Guidance*.)

2.3.2.3 Web Application Containers

Web application containers provide an environment for serving full, interactive application functionality and services on the Web. There are two major container technologies: Java Platform, Enterprise Edition (Java EE) and .NET. NESI expresses no preference regarding which of the two technologies is used; *NESI Part 5: Developer Guidance* addresses both.

The design and implementation of a Node's Web infrastructure should accommodate both Java EE and .NET. The rationale for this is that Nodes will likely have to host services locally and

applications that were developed externally using either technology. Web services (Simple Object Access Protocol or SOAP, XML, etc.) should be used to interoperate between Java EE and .NET applications or services. Such interoperation may be required, for example, when orchestrating Web services across Nodes as part of a Joint mission thread.

As was the case with Web servers, application containers should provide DoD Public Key Infrastructure (PKI) based authentication and role based authorization mapped to certificate attributes as described in the applicable STIGs. Eventually, the container should integrate with the Net-Centric Enterprise Services (NCES) Security Service, described in Section 8.2.2, when available. In the interim, authorization should be based on the Electronic Data Interchange – Personnel Identifier (EDI-PI) contained in the PKI certificate attributes. The use of the EDI-PI as the attribute on which to base authorization decisions is a matter of debate and ongoing engineering, as there are issues about the issuance of EDI-PI to certain user populations, such as coalition users. In the absence of an EDI-PI attribute, other attributes should be used for authorization decisions.

The Web application container should be capable of processing Web services protocols in accordance with the Web Services Interoperability (WS-I) Basic Profile. The container should also support XML security protocols including XML Encryption, XML Signature, and XML Key Management. These protocols are used in protecting content within an XML document that may be passed amongst multiple Web services that are orchestrated. Specific development guidance on the development of services on Web application containers is provided in *NESI Part 5: Developer Guidance.*

2.3.3 Host Information Assurance

Host Information Assurance (IA) protections are part of the DoD Information Assurance Strategic Plan, which in turn is a part of the Net-Ready Key Performance Parameter (NR-KPP) that gets assessed during the Joint Capabilities Integration and Development System (JCIDS) acquisition process. Failure to implement host information assurance protections could jeopardize the approval for a Node to operate on the Global Information Grid (GIG).

Guidance

- Implement commercial off-the-shelf (COTS) virus scanning and worm detection software, along with accompanying capabilities for update of software and virus definitions, on each client or server hardware in the Node in accordance with the Desktop Applications STIG. [G1622]

- Implement personal firewall software on client or server hardware used for remote connectivity in accordance with the Desktop Applications STIG, Network STIG, and Enclave STIG. [G1623]

- Install anti-spyware on all client and server hardware. [G1624]

2.3.4 Domain Directories

Within and across Nodes, directory technologies such as Microsoft's Active Directory (AD) or OpenLDAP are used as tools for system, network, and security administration. Many options exist on how Nodes employ these tools; however, interoperability issues can arise between

Global Information Grid (GIG) Nodes if sub-enterprises employ these tools differently (even within the same technology family, such as AD).

Guidance on Active Directory implementation is being formed by the DoD Active Directory Interoperability Working Group (DADIWG).

Active Directory (AD), if used, implement in accordance with the recommendations of the DADIWG; also, periodically monitor the DADIWG Web site (user authorization required) for the status of GIG implementation issues.

Best Practice

- Implement a Node that uses Active Directory (AD) in accordance with the recommendations of the DoD Active Directory Interoperability Working Group (DADIWG). [BP1679]

2.3.5 Instrumentation for Metrics

Performance has an impact on net-centric operations. Instrumentation is a term frequently used in association with the generation, collection, and analysis of performance metrics. In a dynamic environment, where services and information exchange partners may be dynamic, metrics can be a key factor in the selection of services. Performance metrics that are advertised externally and frequently updated allow potential service users the ability to select an implementation that meets their performance requirements, such as a measurement of reliability. Metrics are normally also needed to ensure performance is provided according to more traditional Service Level Agreements (SLAs), and for operations management.

Component services that are exposed to the Global Information Grid (GIG) by a Node should be instrumented to collect performance metrics. Metrics should be visible and accessible as part of the Component service registration and updated periodically. Standards for metrics are not defined by expected at some point in the future by appropriate GIG working groups.

Some sample metrics that may be appropriate for Web services are in the following table:

SLA Metric	Metric Description
Availability	How often is the service available for consumption?
Accessibility	How capable is the service of serving a client request now?
Performance	How long does it take for the service to respond?
Compliance	How fully does the service comply with stated standards?
Security	How safe and secure is it to interact with this service?
Energy Efficiency	How energy-efficient is this service for mobile applications?
Reliability	How often does the service fail to maintain its overall service quality?

Best Practices

- Instrument Component services that a Node exposes to the Global Information Grid (GIG) to collect performance metrics. [BP1680]

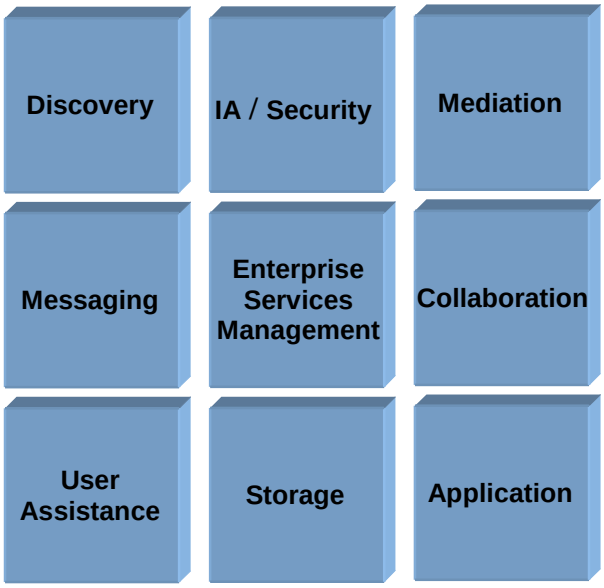
- Make Component services metrics visible and accessible as part of the service registration and updated periodically. [BP1681]

2.4 Node Application Enterprise Services

The DoD has developed an Enterprise Services Strategy that obligates Nodes to employ Enterprise Services to achieve net-centric information sharing. The ultimate goal is to connect people or systems that need information with people or systems that have the needed information. In the strategy, information is considered to be data and/or services. The connection between the information providers and information consumers is the through the use of core enterprise capabilities. Within the DoD, DISA has been chartered to define and develop these capabilities through a project called Net-Centric Enterprise Services (NCES). NCES has the following vision:

> *NCES will enable the secure, agile, robust, dependable, interoperable data-sharing environment for DoD where warfighter, business, and intelligence users share knowledge on a global network that facilitates information superiority, and accelerates decision-making, effective operations, and net-centric transformation.*

In order to accomplish this interconnectivity, NCES has identified nine capabilities that are mapped to services. Collectively, these services are called the Core Enterprise Services (CESs).



Discovery Search, locate or publish data (content), other capabilities (services), or users across the Global Information Grid (GIG).

IA/Security	Authorizes and authenticates Global Information Grid (GIG) users to ensure the confidentiality and integrity of information and services.
Mediation	Translates, brokers, aggregates, fuses or integrates data into commonly understood formats.
Messaging	Distributed, machine-to-machine messaging for notifications and alerts.
Enterprise Service Management	Monitor/manage Global Information Grid (GIG) Enterprise Services against operational performance parameters to ensure reliability and availability of critical capabilities.
Collaboration	Allows users to work together securely on the network by way of video, audio, text chat, white boarding, online meetings, work groups, application sharing.
User Assistance	Provides automated "helper" capabilities and user preferences to help maximize user efficiency in task performance.
Storage	Provides physical and virtual places to host and retain data for purposes such as content staging, continuity of operations, or archival.
Application	Provides the resources necessary to provision, operate and maintain Net-Centric Enterprise Services (NCES) capabilities.

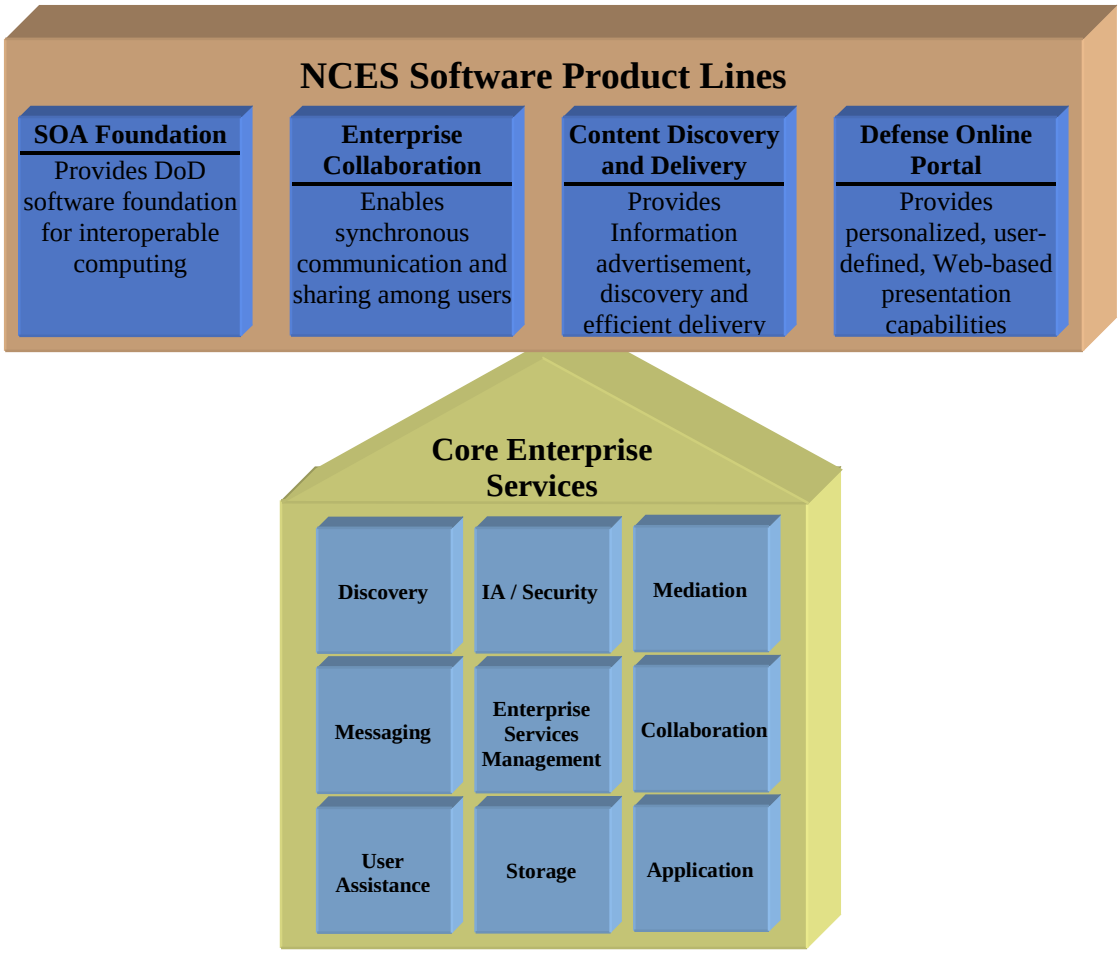
The nine CES are being developed for the entire GIG enterprise by NCES. NCES is using a Software Product Line (SPL) approach to facilitate the building of the CES. The Software Engineering Institute (SEI) defines SPL as follows:

> *A software product line (SPL) is a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way. Software Engineering Institute*

NCES has divided the problem into four product lines:

SOA Foundation	Provides the DoD software foundation for interoperable computing
Enterprise Collaboration	Enables synchronous communication and sharing among users.
Content Discovery and Delivery	Provides Information advertisement, discovery and efficient delivery
Defense Online Portal	Provides personalized, user-defined, Web-based presentation capabilities.

The CES services will be provisioned by DISA and operated on the Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) global networks, initially operating from DISA Enterprise Computing Centers (DECCs).



The CES and SPL approach is very flexible. As a consequence, the exact mechanism of how CES services are employed by Nodes is a topic of active discussions. Overarching issues include maturity, availability, disconnected operations, cross-domain security, and compliance, as described briefly below.

- Overarching Issues
- Core Enterprise Services (CES)
- Community of Interest (COI) Services

2.4.1 Overarching Issues

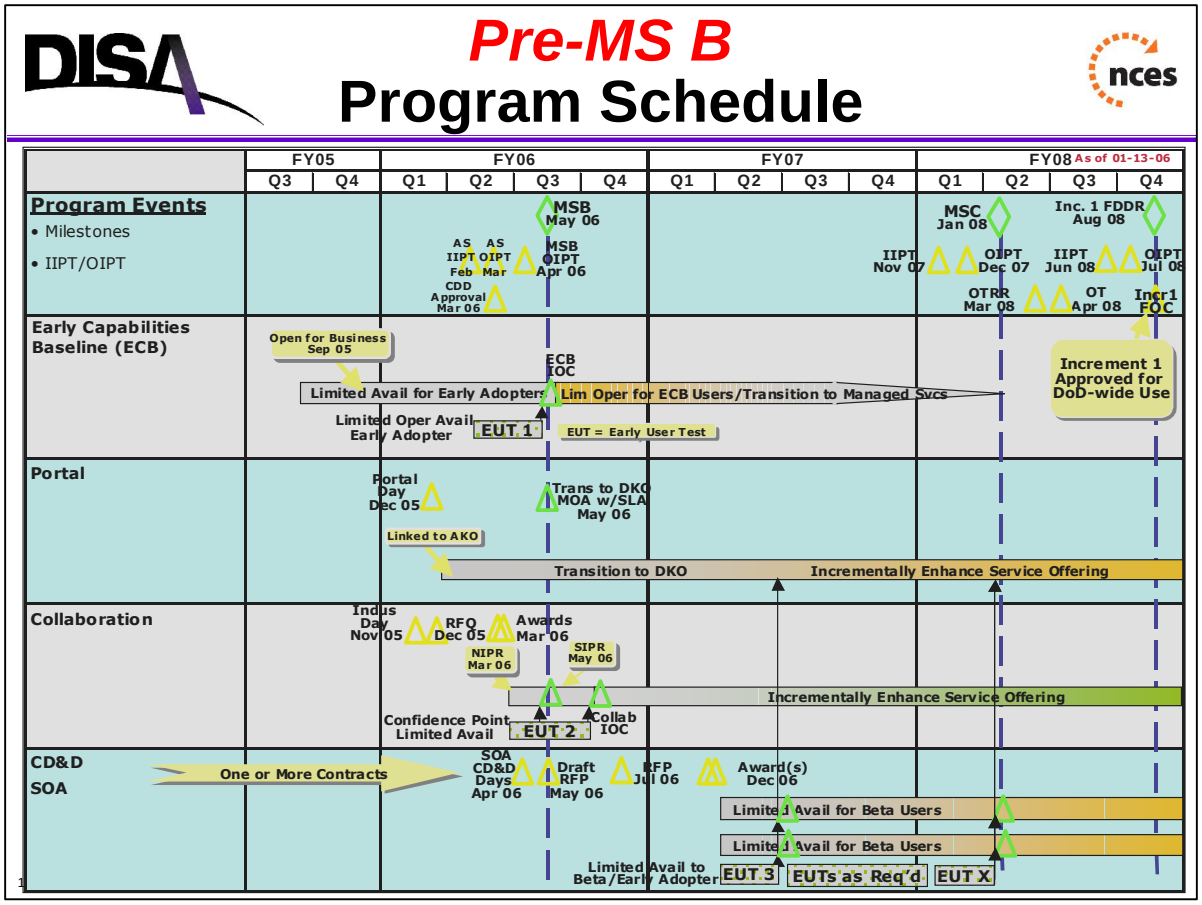
Overarching issues include maturity, availability, disconnected operations, cross-domain security, and compliance. Overarching issues have been divided into the following elements:

- CES Definitions and Status
- CES Parallel Development

- CES and Intermittent Accessibility
- Cross-Domain Interoperation
- Key Interface Profile (KIP) Compliance
- Net-Ready Key Performance Parameter (NR-KPP)
- Core Enterprise Services (CES)

2.4.1.1 CES Definitions and Status

The CES capabilities are in various states of maturity. The Net-Centric Enterprise Services (NCES) program is currently scheduled for a Milestone B decision in the third quarter of 2006.



Capabilities will be delivered in increments; CES Increment 1 capabilities, shown below, are scheduled for operation beginning in 2008 (source: https://ges.dod.mil/soa.htm).

Service Discovery Provides a "yellow pages," categorized by DOD function, enabling users to advertise and locate capabilities available on the network.

Service Security Provides a layer of defense in depth that enables protection, defense, and integrity of the information environment.

Identity Management	Provides the methodology and functions for maintaining information on people, consumers, and service providers. Supports the validation of identity authentication credentials.
Service Management	Enables monitoring of DOD Web services. Provides reporting of service-level information to potential and current service consumers, program analysts, and program managers.
Service Mediation	Allows disparate applications to work together across the enterprise by supporting the transformation of information from one format to another, and the correlation and fusion of data from diverse sources. Supports creation and implementation of process workflows across the enterprise.
Machine-to-Machine Messaging	Provides reliable machine-to-machine message exchange across the enterprise.
Metadata Services	Provides access to Extensible Markup Language (XML) data elements, taxonomy galleries, schemas, and validation and generation tools for DOD software developers.
DOD Web Services Profile	Provides specifications and implementation guidelines to maximize interoperability across DOD Web service implementations.

NCES Increments will be rolled out every 24-26 months. The NCES increment schedule should be considered in scheduling Node evolution, in coordination with systems within the Node.

Guidance

- Provide an environment to support the development, build, integration, and test of net-centric capabilities. [G1576]
- Identify which Core Enterprise Services (CES) capabilities the Node Components require. [G1626]
- Identify the priority of each Core Enterprise Services (CES) capabilities the Node Components require. [G1627]
- Identify which Net-Centric Enterprise Services (NCES) capabilities the Node requires. [G1628]
- Identify which Net-Centric Enterprise Services (NCES) capabilities the Node requires during deployment. [G1629]

Best Practices

- Engage with the Net-Centric Enterprise Services (NCES) program office to explore approaches for mobile use of the Core Enterprise Services (CES) services in mobile Nodes that rely on Transmission Control Protocol/Internet Protocol (TCP/IP) for inter-node communication. [BP1661]

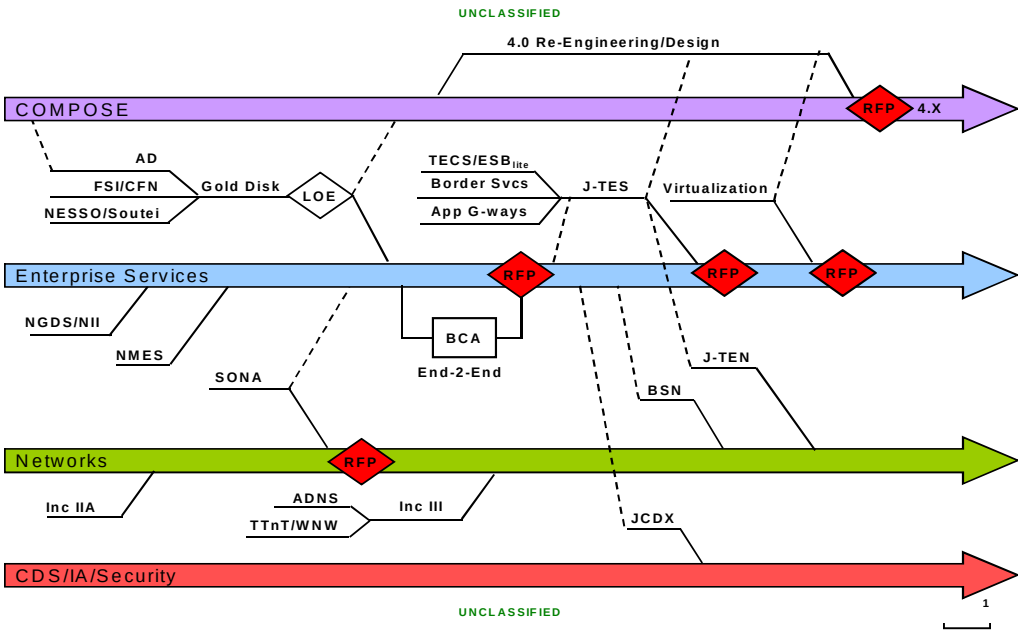
- In the Node's Web infrastructure, support the technologies and standards used by the CES services under development as well as any technologies and standards used for Community of Interest (COI) services. [BP1675]

- Coordinate the Node schedule with the Net-Centric Enterprise Services (NCES) schedule. [BP1683]

- Coordinate the Node schedule with the Component schedules. [BP1684]

Example

The following is an example of how a Service-Oriented Architecture (SOA) Roadmap could be developed by the Navy PEO C4I & Space Networks, IA and Enterprise Services Program Management Office (PMW160) for a project called COMPOSE. The Roadmap lays out the deliveries for four layers: COMPOSE itself, Enterprise Services, Networks, and Security. The milestones and the availability and interdependences of the various parts are documented.



2.4.1.2 CES Parallel Development

Availability of the CES services will be a continuing challenge until all services reach full maturity and operational status. The following table is taken from the Net-Centric Enterprise Services (NCES) workspace of the Defense Online Web site and shows the availability of services comprising the NCES Discovery capability. Designating a CES liaison should help to monitor the availability of CES functionality and report on them back through the engineering

processes of the Node and Components within the Node. Conversely, the engineering processes for the Node and Components should specifically include provisions for incremental implementation of the CES services.

To accelerate the maturation and implementation of the CES, DISA established an *Early Adopter* process. Early adopters can participate in service pilots, as described in the *NCES Pilot Participants Guide*.

Use the early adopter process and service pilots to accelerate implementation of the CES within the Node. Many factors influence the decision to participate in the early adopter process and pilots including acquisition phase, funding, mission, and priorities for individual systems as well as the aggregate Node. Develop a Node-specific service implementation plan.

Nodes operating at special classification levels should coordinate with other Nodes within the same level and with DISA to host CES services on the relevant networks.

Guidance

- Maintain an enterprise service schedule for interim and final enterprise capabilities within the Node. [G1577]
- Define a schedule for Components that includes the use of the Enterprise Services defined within the Node's Enterprise Service schedule. [G1578]
- Identify the priority of each Core Enterprise Services (CES) capability Node Components require. [G1627]
- Specifically include provisions for incremental implementation of the CES services. [G1649]
- Specifically include provisions for incremental implementation of the hosting Node's CES services for Node Components. [G1650]

Best Practices

- Coordinate the Node schedule with the Net-Centric Enterprise Services (NCES) schedule. [BP1683]
- Coordinate the Node schedule with the Component schedules. [BP1684]
- Coordinate with other Nodes having the same compartmentalization needs and with DISA to host compartmentalization CES. [BP1694]
- Designate a CES liaison to monitor the availability of services. [BP1695]
- Use the Early Adopter process and service pilots to accelerate implementation of the CES services within the Node. [BP1696]
- Make the parallel development of CES outside the control of the Node a part of the Node's risk management activities. [BP1697]

2.4.1.3 CES and Intermittent Availability

There are two related challenges: how to handle lapses in the availability of CES services and how to align inter-Node and intra-Node solutions. CES services may be unavailable for several reasons, including loss of connectivity, actual service unavailability, or service rejection. The lack of availability of CES services must not disrupt intra-node availability of locally hosted services. While alignment of intra- and inter-node technical solutions is very desirable, the interface to locally hosted Components must not be dependent on the availability of CES services.

Specific guidance is largely dependent upon the specific Node operating environment and mission. There appear to be some basic options for meeting these challenges:

- Locally host failover copies of certain CES services. Components that are dependent upon Enterprise Services for infrastructure functions, such as security, continue to operate after failing over to the local instances until enterprise accessibility is re-established. This approach requires replication of enterprise services data (the data used by the enterprise services) between the local failover services and the "master" enterprise services. It also requires development of failover behavior in the applications, services, and infrastructure.

- Develop Components to be adaptive, applying default rules and behaviors when Enterprise Services are inaccessible. This approach, along with the definition of the default rules and behaviors would depend on factors such as the sensitivity and importance of the information involved. For example, access control decisions might default to local capabilities such as Active Directory local user accounts. Or local caching might be used to retain the most recently known values for information such as previously discovered services.

- Employ separate external-facing and internal-facing implementations of published services so that external disruptions do not affect local accessibility. The external-facing copy of the service could use Enterprise Services, and the internal-facing copy could implement local Node behavior. As an example, the external-facing copy could implement Public Key Infrastructure (PKI) authentication and authorization, whereas the internal-facing copy could implement Active Directory security. The challenge in this approach is in the coordination of the external-facing and internal-facing copies of such services, such as to provide shared access to databases or replication of data between the external-facing and internal-facing implementations.

Nodes and Components will likely employ some combination of, or evolution of, the above options.

Uniformity and alignment between the technical mechanisms for accessing local services and Enterprise Services should be an objective. Where possible, the burden of providing such uniformity and alignment should rest on the Node infrastructure, rather than the individual Components within the Node, thus isolating the complexities and making them more manageable. Consider the necessity of using CES-provided SDKs and Key Interface Profile (KIP) compliance when formulating an approach; use of an approved SDK may drive separation of external-facing and internal-facing implementation described in the last option above. Finally,

the immaturity of the CES services and the alignment of local and external services access, as a whole, should figure prominently in the risk management activities of the Node and Components within the Node.

Guidance

- Comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) for implemented Core Enterprise Services (CES) in the Node. [G1630]

- Expose Core Enterprise Services (CES) that comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) in all Node services proxies. [G1631]

- Do not implement server side CES functionality for Components. [G1651]

2.4.1.4 Cross-Domain Interoperation

By and large, the implementation of net-centric concepts across security domains has not been defined. Trusted guards do not act as network routers; information to be transferred across a guard is delivered to the guard, processed, and then delivered to a defined endpoint on the other side if the rules are satisfied. The guard in the middle disrupts the normal pattern for use of the CES services.

In order for services to work through the trusted guards that interconnect different domains, there must be a well defined set of messages that can be passed through the guard to effect the conversation necessary to use the service and return results. This restriction, if built into the service's interface, could be unduly restrictive on the design of the interface.

It may be more practical for each such service to provide service proxies for use in the other security domains, and corresponding client proxies in the local domain. The server proxy and client proxy for the service might then communicate across the trusted guard in a private, high efficiency manner that the guard can process. But even this approach is restrictive in that the server proxies have to be installed in the other security domains, and this departs from some fundamentals of net-centric concepts such as dynamic service discovery.

Until such approaches are prototyped and explored more fully, Nodes should anticipate that services will not be capable of cross-domain invocation. Furthermore, for services that have utility in other security domains, implementer should consider providing copies of such services for hosting in the other domains, and use XML document transfers across the trusted guard to keep the copies in synchronization. This approach depends on many factors, and may not be suitable for all services.

Guidance

- Prepare a Node to host new Component services developed by other Nodes or by the enterprise itself. [G1613]

- Prepare a Node for the possibility of becoming a new Component service within another Node. [G1614]

Best Practices

- Use Node implemented Service Discovery (SD) to meet compartmentalization needs. [BP1691]

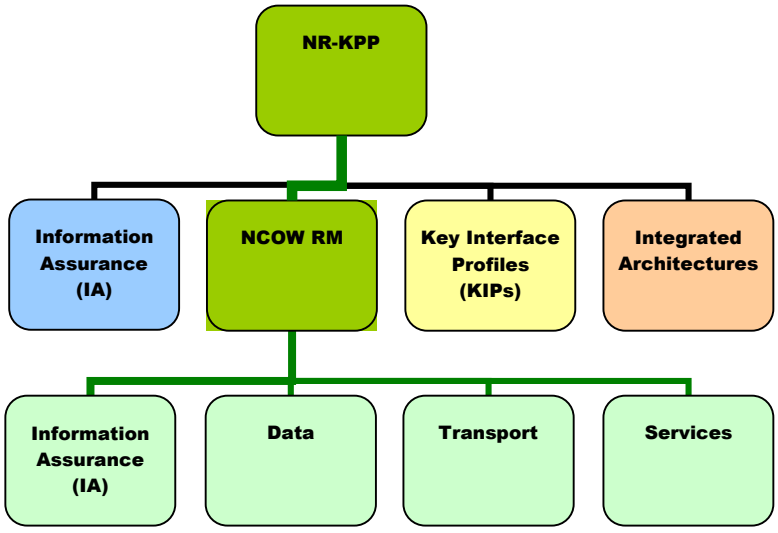
- Do not expect cross-domain invocation of Component services within a Node. [BP1698]

2.4.1.5 Net-Ready Key Performance Parameter (NR-KPP)

The following information is from the Defense Acquisition University (DAU) Defense Acquisition Guidebook, Chapter 7.3.4. The Net-Ready Key Performance Parameter (NR-KPP) has been developed to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP replaces the Interoperability KPP, and incorporates net-centric concepts for achieving Information Technology (IT) and National Security Systems (NSS) interoperability and supportability. The NR-KPP assists Program Managers, the test community, and Milestone Decision Authorities in assessing and evaluating IT and NSS interoperability.

The NR-KPP assesses information needs, information timeliness, information assurance, and net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. The NR-KPP consists of verifiable performance measures and associated metrics required to evaluate the timely, accurate, and complete exchange and use of information to satisfy information needs for a given capability. Program managers will use the NR-KPP documented in Capability Development Documents (CDD) and Capability Production Documents (CPD) to analyze, identify, and describe IT and NSS interoperability needs in the Information Support Plan (ISP) and in the test strategies in the Test and Evaluation Master Plan.

The following diagram explains the relationships of the Global Information Grid (GIG) Key Interface Profiles (KIPs), Net-Centric Operations and Warfare Reference Model (NCOW RM), ASD(NII) Net-Centric Checklist, and the Net-Ready Key Performance Parameter (NR-KPP).



- Information Assurance (IA)
- Net-Centric Operations and Warfare Reference Model (NCOW RM)

- Key Interface Profile (KIP)
- Integrated Architectures

References

- See the following items from the Defense Acquisition Guidebook:
  - Compliance with the Net-Centric Operations and Warfare Reference Model
  - Compliance with applicable Global Information Grid Key Interface Profiles
  - Compliance with DoD Information Assurance requirements
  - Supporting integrated architecture products

2.4.1.6 Information Assurance (IA)

Most Nodes delivering capability to the warfighter or business domains will use Information Technology (IT) to enable or deliver that capability. For those Nodes, developing a comprehensive and effective approach to IA is a fundamental requirement and is key in successfully achieving Node's objectives. The DoD defines IA as follows:

> *Information Assurance (IA) are the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.*

DoD policy and implementing instructions on information assurance are in the 8500 series of DoD publications. Nodes and Components for programs should be familiar with statutory and regulatory requirements governing information assurance and understand the major tasks involved in developing an IA organization, defining IA requirements, incorporating IA in the Node's and Component architecture, developing an acquisition IA strategy (when required), conducting appropriate IA testing, and achieving IA certification and accreditation for the program.

Guidance

- Certify and accredit Nodes with all applicable DoD Information Assurance (IA) processes. [G1632]

- Host only DoD Information Assurance (IA) certified and accredited Components. [G1633]

- Certify and accredit Components with all applicable DoD Information Assurance (IA) processes. [G1634]

References

- DoD Directive 5000.1, Enclosure 1, Paragraph E1.9, Information Assurance

  Acquisition managers shall address information assurance requirements for all weapon systems; Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance systems; and information technology programs that depend on external information sources or provide

information to other DoD systems. DoD policy for information assurance of information technology, including NSS, appears in DoD Directive 8500.1….

- DoD Instruction 5000.2, Enclosure 4, Paragraph E.4.2, IT System Procedures states, "The program defines the requirement for an Information Assurance Strategy for Mission Critical and Mission Essential IT systems."

  The DoD CIO must certify (for MAIS programs) and confirm (for MDAPs) that the program is being developed in accordance with the CCA before Milestone approval. One of the key elements of this certification or confirmation is the DoD CIO's determination that the program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.

- DoD Instruction 5000.2, Enclosure 4, Table E4.T1, CCA Compliance Table: requires that "[t]he program has an information assurance strategy that is consistent with DoD policies, standards and architectures, to include relevant standards.

- DoD Directive 8500.1, "Information Assurance (IA)": This directive establishes policy and assigns responsibilities under 10 U.S.C. 2224 to achieve Department of Defense information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to net-centric warfare.

- DoD Instruction 8500.2, "Information Assurance (IA) Implementation": This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoD Directive 8500.1.

- DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System": This instruction implements policy, assigns responsibilities, and prescribes procedures necessary to integrate Information Assurance (IA) into the Defense Acquisition System; describes required and recommended levels of IA activities relative to the acquisition of systems and services; describes the essential elements of an Acquisition IA Strategy, its applicability, and prescribes an Acquisition IA Strategy submission and review process.

- DoD Instruction 5200.40, "DoD Information Technology Security Certification And Accreditation Process (DITSCAP)": This instruction implements policy, assigns responsibilities and prescribes procedures under DoD Directive 8500.1 for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in the DoD.

  - According to DoD Directive 8500.1, all acquisitions of Automated Information Systems (AISs), to include Automated Information System applications, outsourced IT-based processes, and platforms or weapon systems with connections to the Global Information Grid (GIG) must be certified and accredited according to DoD Instruction 5200.40, DITSCAP.

- See other applicable Certification & Accreditation processes (such as Director of Central Intelligence Directive (DCID) 6/3 "Protecting Sensitive Compartmented Information within Information Systems" for systems processing Sensitive Compartmented Information).

2.4.1.7 Net-Centric Operations and Warfare Reference Model (NCOW RM)

The Net-Centric Operations and Warfare Reference Model (NCOW RM) represents the strategies for transforming the enterprise information environment of the Department. It is an architecture-based description of activities, services, technologies, and concepts that enable a net-centric enterprise information environment for warfighting, business, and management operations throughout the Department of Defense. Included in this description are the activities and services required to establish, use, operate, and manage this net-centric enterprise information environment. Major activity blocks include the generic user-interface (A1), the intelligent-assistant capabilities (A2), the net-centric service (core, Community of Interest, and enterprise control) capabilities (A3), the dynamically allocated communications, computing, and storage media resources (A4), and the enterprise information environment management components (A5). Also included is a description of a selected set of key standards and/or emerging technologies that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized.

Transforming to a net-centric environment requires achieving four key attributes: reach, richness, agility, and assurance. The initial elements for achieving these attributes include the Net-Centric Enterprise Services (NCES) Strategy, the DoD Net-Centric Data Strategy, and the DoD Information Assurance (IA) Strategy to share information and capabilities. The NCOW RM incorporates (or will incorporate) these strategies as well as any net-centric results produced by the Department's Horizontal Fusion (HF) pilot portfolio.

The NCOW RM provides the means and mechanisms for acquisition program managers to describe their transition from the current environment (described in GIG Architecture Version 1) to the future environment (described in GIG Architecture Version 2). In addition, the NCOW RM will be a key tool during program oversight reviews for examining integrated architectures to determine the degree of net-centricity a program possesses and the degree to which a program can evolve to increased net-centricity. Compliance with the NCOW RM is one of the four elements that comprise the Net-Ready Key Performance Parameter (NR-KPP).

Guidance

- Comply with the Net-Centric Operations and Warfare Reference Model (NCOW RM). [G1636]

2.4.1.8 Key Interface Profile (KIP)

The following information is from the Defense Acquisition University (DAU) Defense Acquisition Guidebook, Chapter 7.3.4.2. A Key Interface Profile (KIP) is the set of documentation produced as a result of interface analysis which designates an interface as key; analyzes it to understand its architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during the analysis. The profile consists of refined operational and systems view products, Interface Control Document/Specifications, Systems Engineering Plan, Configuration

Management Plan, Technical Standards View (TV-1) with SV-TV Bridge, and procedures for standards conformance and interoperability testing. Relevant Global Information Grid (GIG) KIPs, for a given capability, are documented in the Capability Development Document and Capability Production Document. Compliance with identified GIG KIPs are analyzed during the development of the Information Support Plan (ISP) and Test and Evaluation Master Plan, and assessed during Defense Information Systems Agency Joint Interoperability Test Command (JITC) joint interoperability certification testing. An interface is designated as a key interface when one or more the following criteria are met:

- The interface spans organizational boundaries.
- The interface is mission critical.
- The interface is difficult or complex to manage.
- There are capability, interoperability, or efficiency issues associated with the interface.
- The interface impacts multiple acquisition programs.

Program manager compliance with applicable GIG KIPs is demonstrated through inspection of Joint Capabilities Integration and Development System (JCIDS) documentation and test plans, and during JITC interoperability certification testing (see references [j] and [l], CJCS Instruction 3170.01 and CJCS Instruction 6212.01, respectively, for detailed discussions of the process).

KIPs are being defined to specify the interfaces to the Core Enterprise Services (CES). Compliance with these KIPs is a mandatory element of the Net-Ready Key Performance Parameter (NR-KPP). The KIP specifications are in various states of maturity and may be viewed at http://kips.disa.mil (user registration required).

Guidance

- Comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) for implemented Core Enterprise Services (CES) in the Node. [G1630]

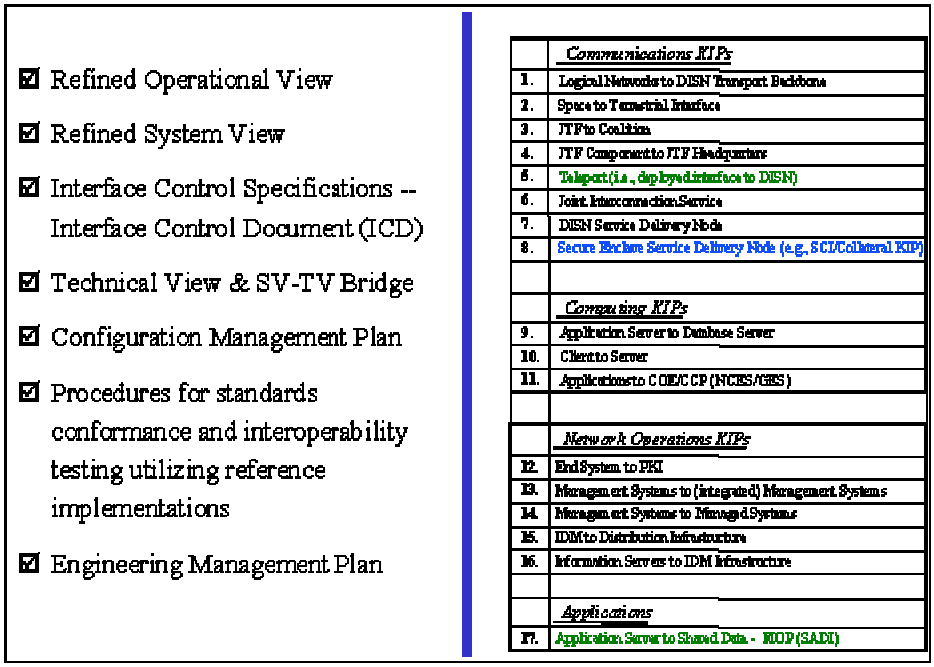
- Expose Core Enterprise Services (CES) that comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) in all Node services proxies. [G1631]

Best Practice

- For Key Interface Profile (KIP) specifications that are not available or insufficiently mature, implement a “best effort” by following the published intent of functionality and monitor or participate in the relevant specification development body. [BP1685]

Example

GIG Key Interface Profiles (KIPs) provide a net-centric oriented approach for managing interoperability across the GIG based on the configuration control of key interfaces.



Reference

- http://akss.dau.mil/dag/Guidebook/IG_c7.3.4.2.asp

2.4.1.9 Integrated Architectures

The DoD Architecture Framework (DoDAF) provides the rules, guidance, and product descriptions for developing and presenting architecture descriptions to ensure a common denominator for understanding, comparing, and integrating architectures. An integrated architecture consists of multiple views or perspectives (Operational View [OV], Systems View [SV], Technical Standards View [TV] and All-Views [AV]) that facilitate integration and promote interoperability across capabilities and among related integrated architectures.

- The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions.
- The SV is a description, including graphics, of systems and interconnections providing for, or supporting, DoD functions.
- The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure that a conformant system satisfies a specified set of requirements.
- The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture.

The GIG architecture describes the basic, high level architecture in which Nodes reside. It is an integrated architecture consisting of the various DoDAF views. It provides a common lexicon and defines a basic infrastructure for the performance of information exchanges with other Global Information Grid (GIG) Nodes using the GIG Enterprise Services (GES) and the Net-Centric Enterprise Services (NCES). The GIG Architecture can be viewed https://disain.disa.mil/ncow/gigv2/index.htm; the home page for both the GIG architecture and

Net-Centric Operations and Warfare Reference Model (NCOW RM) is https://disain.disa.mil/ncow.html (user registration required).

Guidance

- Make Nodes that will be part of the Global Information Grid (GIG) consistent with the GIG Integrated Architecture. [G1635]

References

- DoD Architecture Framework (DoDAF), http://www.defenselink.mil/nii/doc/DoDAF_v1_Volume_I.pdf
- The GIG Architecture, https://disain.disa.mil/ncow/gigv2/index.htm
- The NCOW RM, https://disain.disa.mil/ncow.html

2.4.2 Core Enterprise Services (CES)

- Directory Services
- Security Services
- Services Management
- Service Discovery
- Content Discovery Services
- Mediation Services
- Collaboration Services
- Machine-to-Machine Messaging

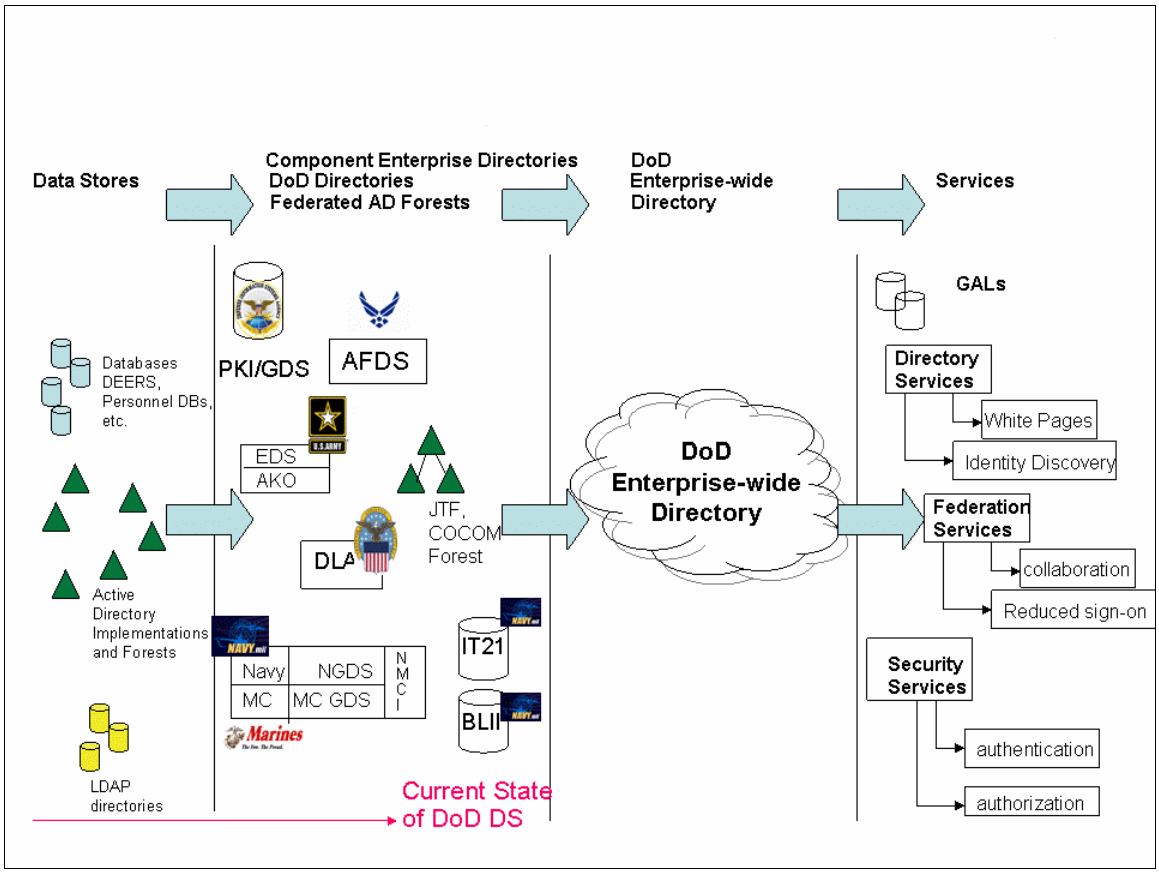
2.4.2.1 Directory Services

Secure inter-node interoperability relies heavily on the ability to lookup information about people and objects or devices across the breadth of the Global Information Grid (GIG). The technology that supports this is called directory services. In the Net-Centric Enterprise Services (NCES) service taxonomy, this falls under the scope of the CES Discovery Service for person and device discovery).

Nodes routinely use directory services today, such as Microsoft Active Directory and the DoD Public Key Infrastructure (PKI) Global Directory Service (GDS). Although implementations are widespread across the GIG, there is limited coordination and synchronization, creating pockets of information that must be unified. There are also substantial differences among implementations, including naming conventions. This situation is made more complex by the fact that these directories are typically also integral to a Node's security and system administration, supporting such basic functions as user login.

Coordination efforts at the level of the GIG within the DoD are underway to address these challenges. The DoD CIO directed DISA to develop a roadmap for directory services for the GIG. That roadmap is in draft form and is the product of the Joint Enterprise Directory Services Working Group (JEDIWG), which maintains a Web site at https://gesportal.dod.mil/sites/JEDIWG/default.aspx. This working group oversees both the Joint Directory Services Working Group (JDSWG) that focuses on PKI related requirements addressed by the Global Directory Service (GDS) as well as the DoD Active Directory

Interoperability Working Group (DADIWG). A snapshot of directory services evolution is in the diagram below:



Guidance

- Provide a commercial off-the-shelf Directory Service that all the Components of a Node can use. [G1625]

- Make Node-implemented directory services comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs). [G1637]

- Comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node directory services proxies. [G1638]

Best Practices

- Align Node interfaces to Components for directory services with the guidance being provided by the JEDIWG and sub-working groups, including such guidance as naming conventions, federation, and synchronization. [BP1686]

- Follow Active Directory naming conventions defined in "Active Directory User Object Attributes Specification," as required by the DoD CIO memorandum, "Microsoft Active Directory (AD) Services." [BP1687]

2.4.2.2 Security Services

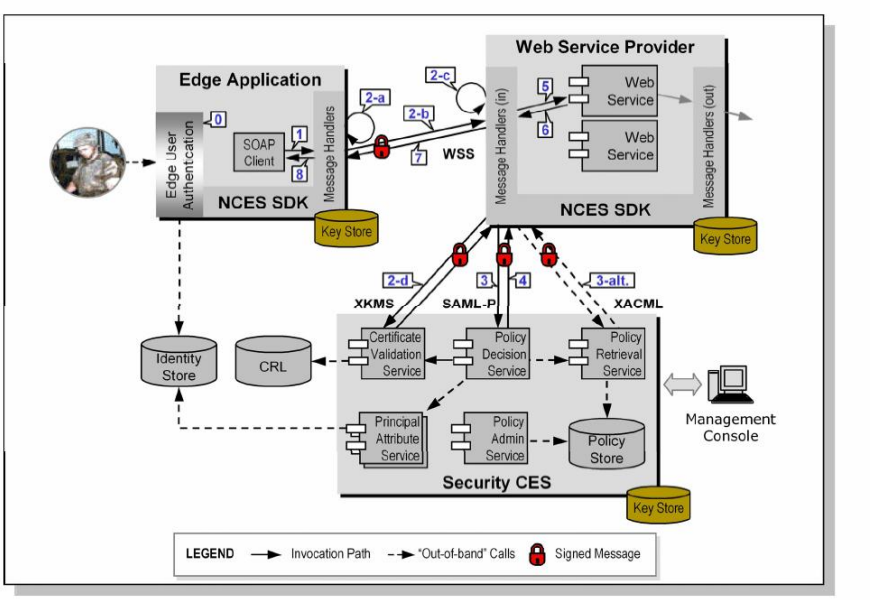
Net-centric information exchanges require security. The security mechanisms must be understood and implemented Global Information Grid (GIG)-wide because the information exchanges may occur between any Nodes on the GIG.

The CES approach to providing these GIG-wide security mechanisms is based on the DoD Public Key Infrastructure (PKI). Several security services in multiple categories of functionality are defined or planned, as shown in the following table. Generally, these services add to the DoD PKI authentication capabilities, providing a more complete set of security capabilities to applications, infrastructure, or other services.

Security Service Categories	Current Services	Future Services
Credential Mgmt Services	Certificate Validation Service	Certificate Retrieval Service Certificate Registration Service
Authorization Services	Policy Decision Service Policy Retrieval Service Policy Administration Service	Policy Subscription Service
Attribute Services	Principal Attribute Service	Resource Attribute Service Environment Attribute Service
Security Context Services	None	Security Context Service
Auditing & Logging Services	None	Security Logging Service Auditing Service

The figure below shows the relationship and typical interactions of these elements for a typical Web client invocation of a Web service. Node implementation of the elements shown below presents some critical design choices. The figure does not show, for instance, where each of the elements found in the "Security CES" box are hosted. There is active debate over this and related topics.

Authorization decisions should be the local purview of the Nodes, based on enterprise standards for identity, attributes, and policies, augmented and tailored locally to suit any unique requirements a Node may have. Furthermore, because security decisions can be computationally intensive and frequent, locally hosted implementations may be warranted by performance. Therefore, CES Security Services for authorization and policy decisions should be hosted locally on a Node. This requires coordination with DISA to implement these services on the local Node, and the overall approach may change as the Security Services are more fully developed and piloted.



Implementation topics for near term consideration are Identity Management, authentication, and authorization.

- Identity Management
- Public Key Infrastructure (authentication, and authorization)

2.4.2.2.1 Identity Management

Identity is an essential part of the CES Security Services, but Identity Management is not addressed in CES Increment 1. Identities of Global Information Grid (GIG) entities, human and non-human (i.e., services), must be unique across the GIG. DoD PKI X.509 certificates reserve a field to contain identity data, but there are issues today with how that field is populated for certain populations of users (e.g., coalition partners), and how to handle non-person entities. These issues are described in the paper entitled "Net-Centric Enterprise Services SOA Foundation Product Line, Service Security Component, Whitepaper: Service Identity Management and Credentialing."

While a universal solution for Identity Management is not yet defined, it is possible to make progress in the implementation of these services, particularly for Web applications and services with U.S. users having a CAC identification card holding DoD PKI X.509 certificates.

Identity is not as well understood and defined for non-person entities, such as services that may be part of a long invocation chain that is part of a workflow or orchestrated to yield a specific answer to a service invocation. Web server credentialing, though, has been defined to rely upon the DNS name of the site for identification.

The Net-Centric Enterprise Services (NCES) and Public Key Infrastructure (PKI) program offices are working on the challenges of non-person Identity Management, and an RFI has been issued to identify potential solutions.

Guidance

- Use DoD PKI X.509 certificates for servers. [G1652]

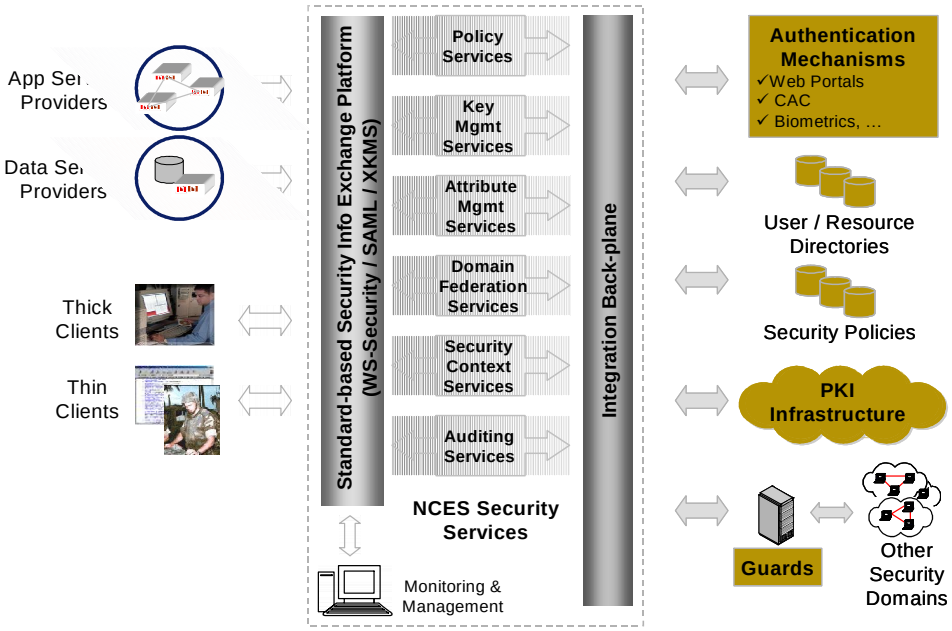
2.4.2.2.2 Public Key Infrastructure

Net-Centric Enterprise Services (NCES) Security Services rely heavily on Public Key Infrastructure (PKI) and Public Key (PK) Enabling (PKE). PKI provides an assured way for enabled applications to authenticate both intra-node and inter-node. PKI supports the concept of a single login across the enterprise, but legacy non-PK-enabled applications and services mean that username and password synchronization is also needed to support the single login concept; however, this is only practical in a limited sense (i.e., not the entire GIG). There remain some PKI implementation challenges, such as the implementation of the process for validating that an entity's certificate has not been revoked. Some COTS products, including some Web Application Containers, do not support the use of the Online Certificate Status Protocol (OCSP) or do not provide a capability to do file-based checking of the older Certificate Revocation List (CRL).

Nodes having both DoD and Intelligence Community (IC) systems and networks will also face the fact that the DoD and IC have implemented separate PKIs (including the dependent Directory Services). In general, the DoD PKI operates on the collateral classification networks, and the IC PKI operates on the SCI classified networks. Nodes may have to interface with multiple PKIs, therefore, depending on the systems and security levels at the Node. This presents some additional challenges when cross-domain interoperation is required, whether intra- or inter-node.

Nodes that have multinational or coalition personnel accessing the system will also encounter a challenge in obtaining CACs containing PKI certificates for these persons. The process is not well defined. As DoD moves further into the net-centric concepts, obtaining certificates for non-human entities in multinational or coalition systems will also be a challenge.

Authorization based on attributes corresponding to an entity is a practical way to implement authorization, provided that the enterprise can agree on the definitions of the attributes, policy, and a way of securely communicating and validating role membership. Unfortunately, attribute definitions and common security policy are not defined yet for the Global Information Grid (GIG), and Nodes are forced to use interim approaches, such as Windows AD or NIS group memberships, and evolve to a uniform definition of GIG roles and policies. Federation has not been addressed sufficiently to provide specific guidance.



2.4.2.3 Services Management

Net-centric operations can create mutual, mission-dependent obligations between Nodes. Service Management affects Node interoperability in that failure to provide services according to advertised capabilities or negotiated Service Level Agreements (SLAs) is essentially non-interoperability in the performance dimension.

Net-Centric Enterprise Services (NCES) services management capabilities are under development, but, as indicated in the current NCES schedule, are not scheduled for fielding until CES Increment 2.

Best Practice

- For Services Management, use an interim solution of instrumentation of services and external monitoring. [BP1688]

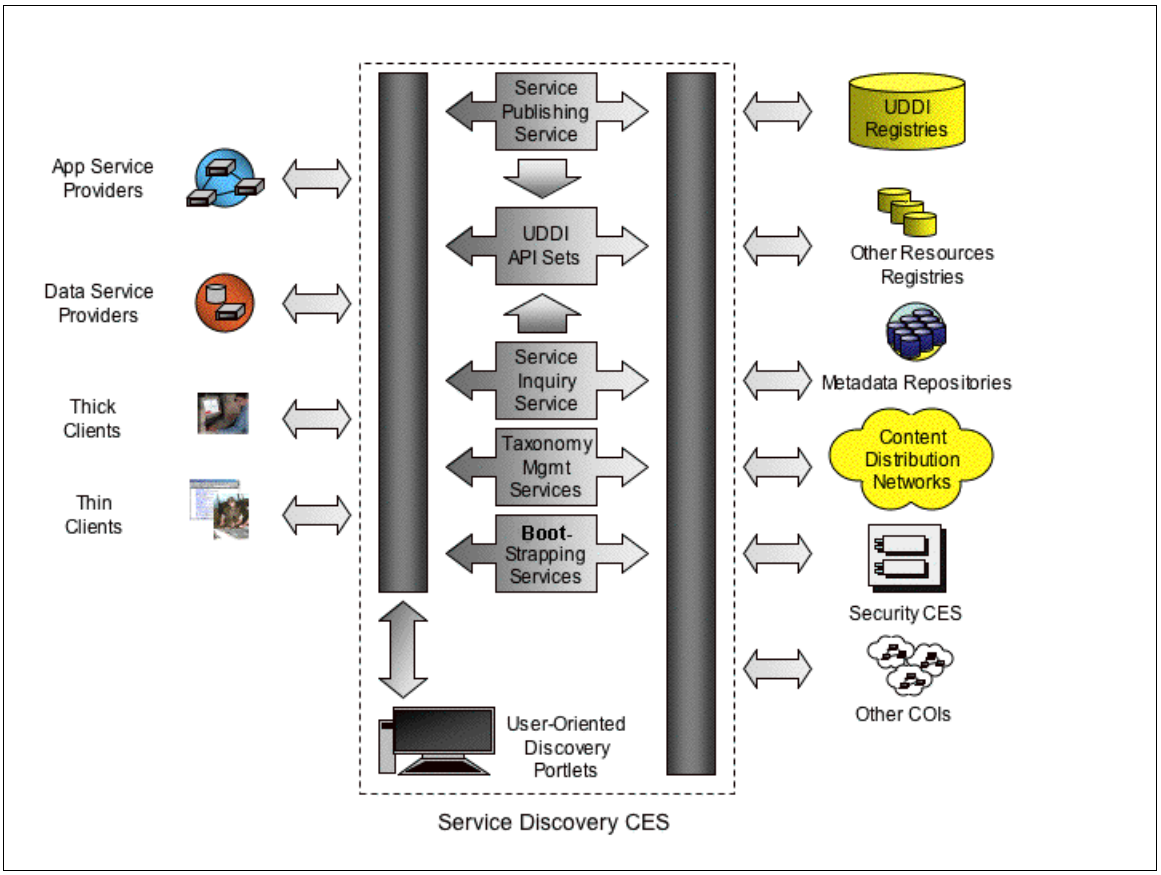
2.4.2.4 Service Discovery

Loosely coupled, net-centric information and services must be discoverable. That is, Nodes and Components must be able to discover dynamically where Component services and information reside in the Global Information Grid (GIG) and bind to those providers at runtime. The discovery concept relies upon the use of registries that are human and machine usable, for maintaining meta-data descriptions of information and services.

In Net-Centric Enterprise Services (NCES), service discovery is implemented by the CES Service Discovery (SD) services. Scheduled for CES Increment 1 fielding, a pilot implementation of SD services is available. The construction of registry entries is specified by the Service Definition Framework (SDF). The following figure shows the overall SD services architecture. Web portlets are being developed to assist in using the service, providing support for service publishing, searching, and browsing. The service registry implementation uses the Universal Description, Discovery, and Integration (UDDI) registry underneath, and the portlets

use the UDDI application programming interface (API). A Service Discovery Portlet Users Guide describes how to use the portlets to access the registry.

Nodes again face several implementation choices regarding alignment of Components and Nodes approaches. Components exposed by the Node should be described as specified by the SDF and registered with the DISA hosted registries so that the Components services are visible to other Nodes. The pilot program should be used to practice and exercise the mechanics of service discovery and late binding. If the pilot implementation is not reachable, such as might be the case in a higher classified environment, the Node managers should coordinate amongst themselves and DISA to provide pilot and full service implementations that are reachable. Internal-facing services that are not likely to be of value beyond the Node's boundaries do not have to be discoverable, though it is a recommended best practice. If used internally, though, service discovery should be implemented for high availability.



Guidance

- Describe Components exposed by the Node as specified by the Service Definition Framework (SDF). [G1639]
- Register components exposed by the Node with the DISA-hosted registries. [G1640]
- Comply with the Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node-implemented Service Discovery (SD). [G1641]

- Comply with the Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node Service Discovery (SD) proxies. [G1642]

Best Practices

- Use the Service Discovery (SD) pilot program to practice and exercise the mechanics of service discovery and late binding. [BP1689]

- Use Node implemented Service Discovery (SD) for high availability. [BP1690]

- Use Node implemented Service Discovery (SD) to meet compartmentalization needs. [BP1691]

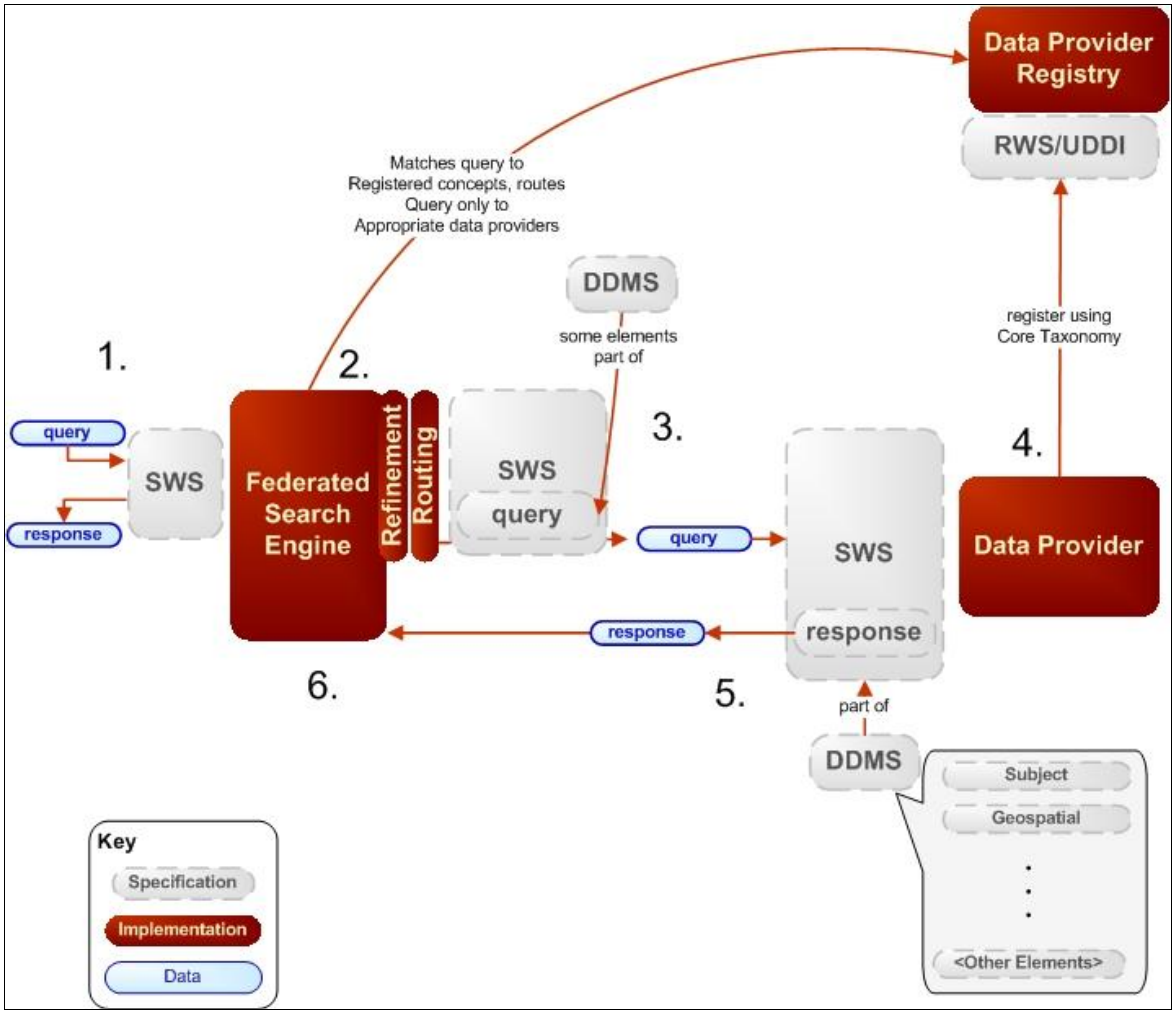
2.4.2.5 Content Discovery Services

Net-Centric Enterprise Services (NCES) includes a Content Discovery Service (CDS) that provides a Federated Search capability. That is, the service can search across a set of Content Discovery Services and yield an integrated result. The current approach to providing this service is to harness an existing capability termed "Federated Search" developed under the Horizontal Fusion (HF) program. The capability utilizes the DoD Discovery Metadata Specification (DDMS).

The Federated Search and DDMS document contains the following information:

> *Federated Search is implemented as a set of cooperating Web services. These services talk to each other using a common specification. The specification defines how a query and the results from that query are communicated. It describes not only the meaning, but also the format of the data that is exchanged between the services.*
>
> *The Defense Discovery Metadata Specification (DDMS) is used in the Federated Search specification to represent the concepts of a query as well as the resource result records, called meta cards, generated by a search result. Outgoing queries are matched against the resource meta cards by data providers to generate search results. It is the DDMS that ties the queries to the results and is used to express a common vocabulary.*

The following figure shows the Horizontal Fusion program's implementation of this Federated Search capability. Each Node should implement Federated Search - Registration Web Service (RWS) and Search Web Service (SWS). The RWS is used by data producers to register content sources and the SWS is used to search for content from the registered sources.



Guidance

- Comply with the Federated Search – Registration Web Service (RWS) Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node implemented Federated Search – Registration Web Service (RWS). [G1643]

- Comply with the Federated Search – Search Web Service (SWS) Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node implemented Federated Search – Search Web Service (SWS). [G1644]

- Implement a local Content Discovery Service (CDS). [G1645]

- Comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node Federated Search Services proxies. [G1646]

- Provide access to the Federated Search Services. [G1647]

- Host the Registration Web Service (RWS) registration portlet in the Node. [G1648]

2.4.2.6 Mediation Services

Published information may not always be in a format compatible with the subscriber's needs. The CES Mediation Service currently provides a capability to translate XML documents from one schema into another. To do this, the service uses Extensible Stylesheet Language Transformations (XSLT) and mappings DoD Metadata Registry. When XML document translation between schemas is a necessity, use the CES Mediation Service or a locally hosted copy thereof. Register developed mappings in the DoD Metadata Registry. (For additional information, see the Mediation Services perspective in *NESI Part 5: Developer Guidance*).

Best Practices

- Use the CES Mediation Service, or a locally hosted copy, when XML document translation between schemas is a necessity. [BP1711]

- Register developed mappings in the DoD Metadata Registry. [BP1712]

2.4.2.7 Collaboration Services

Collaboration tools provide a virtual meeting room environment for human interaction. The virtual environment enables multimedia collaboration (text, voice, and video) in multiple modes (person-to-person, open chat, restricted meeting, etc.) and application broadcasting and sharing.

A suite of collaboration tools and standards called the Defense Collaboration Tool Suite (DCTS) has been validated for interoperability by the DISA Joint Interoperability Test Command (JITC) and is used operationally. The DCTS Collaboration Management Office (CMO) within DISA is responsible for fielding, sustaining, and managing the life cycle of DCTS. Collaboration products approved for interoperability are listed at http://jitc.fhu.disa.mil/washops/jtcd/dcts/dctsv2_software_list.html. Products certified for use on Secret Internet Protocol Router Network (SIPRNET) are listed at http://jitc.fhu.disa.mil/washops/jtcd/dcts/projects.html.

Net-Centric Enterprise Services (NCES) will provide a Collaboration Service. A pilot of a Next Generation Collaboration Service (NGCS) was recently concluded and has resulted in a Collaboration Service Request for Quotation (RFQ). The RFQ can be viewed at https://www.ditco.disa.mil/dcop/public/asp/requirement.asp?req_no=NCES_COLLABRFQ. This RFQ states an intention to select two competitive vendors for both the NIPRNET and SIPRNET communities, allowing users a choice of services. Provisions are also made within the RFQ for Offerors to propose solutions for providing service in degraded environments, such as low bandwidth, and in other networks and separated enclaves. It is possible for services to be operational during 2006. The schedule indicates that progress on fielding the Collaboration Service should be monitored closely in the near term, and take steps to determine actively which vendor offering to employ (perhaps hosting at the Node) if in a disadvantaged environment or separate network.

The recent DOD CIO memorandum, "DoD Collaboration Policy Update," requires use of the NCES Collaboration Services that are under development. It also provides policy for urgent requirements until the NCES services are operational. Collaboration products used to satisfy urgent requirements should be approved and from the list on the aforementioned Web sites, until the NCES Collaboration Service is available.

Best Practices

- The schedule indicates that progress on fielding the Collaboration Service should be monitored closely in the near term; take steps to determine actively which vendor offering to employ (perhaps hosting at the Node) if in a disadvantaged environment or separate network. [BP1692]

- Make sure that collaboration products used to satisfy urgent requirements are from the JTIC list (see http://jitc.fhu.disa.mil/washops/jtcd/dcts/dctsv2_software_list.html and, for products certified for use on SIPRNET, http://jitc.fhu.disa.mil/washops/jtcd/dcts/projects.html) until the Net-Centric Enterprise Services (NCES) Collaboration Service is available. [BP1693]

2.4.3 Machine-to-Machine Messaging

Net-Centric Enterprise Services (NCES) is defining services for machine-to-machine messaging, similar in capability to services offered by several COTS vendors of Enterprise Service Busses (ESBs). ESBs, though, are not yet interoperable enough to support messaging between arbitrary Global Information Grid (GIG) Nodes using different ESBs. NESI guidance is TBD until this service is better defined.

Glossary

Term	Acronym	Definition
Access Control List	**ACL**	In computer security, ACL is a concept used to enforce privilege separation. It is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request, principally the process's user identity. In networking, ACL refers to a list of ports and services that are available on a host, each with a list of hosts and/or networks permitted to use the service. Both individual servers as well as routers can have access lists. Access lists are used to control both inbound and outbound traffic, and in this context they are similar to firewalls. http://en.wikipedia.org/wiki/Access_control_list
Active Directory	**AD**	An implementation of Lightweight Directory Access Protocol (LDAP) directory services by Microsoft for use in Windows environments; allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization. An Active Directory stores information and settings relating to an organization in a central, organized, accessible database. Active Directory networks can vary from a small installation with a few hundred objects, to a large installation with millions of objects. http://en.wikipedia.org/wiki/Active_Directory
All-Views	**AV**	The DoDAF All-Views (AV) products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and timeframe for the architecture. The setting in which the architecture exists comprises the interrelated conditions that compose the context for the architecture. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions. DoDAF v1 Vol. 1, 9 Feb 2004, page 1-3, section 1.3.4

Term	Acronym	Definition
Application		Provides the resources necessary to provision, operate and maintain Net-Centric Enterprise Services (NCES) capabilities.
Assistant Secretary of Defense for Networks and Information Integration	**ASD/NII**	The Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) is also the DoD Chief Information Officer (CIO).
Browser		Short for *Web browser,* a software application used to locate and display Web pages. http://www.webopedia.com/TERM/b/browser.html
Capability Development Document	**CDD**	A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of militarily useful, logistically supportable and technically mature capability. CJCSI 3170.01E, 11 May 2005, Glossary page GL-5
Capability Production Document	**CPD**	A document that addresses the production elements specific to a single increment of an acquisition program. CJCSI 3170.01E, 11 May 2005, Glossary page GL-5
Certificate		In computing and especially computer security and cryptography, the word *certificate* generally refers to a digital identity certificate, also known as a Public Key (PK) certificate. It also may be awarded as a necessary certification to validate that a student is considered competent in a certain specific networking skill area in today's ubiquitous and necessary Information Technology (IT). http://en.wikipedia.org/wiki/Certificate
Certificate Revocation List	**CRL**	A list of certificates (more accurately: their serial numbers) which have been revoked, are no longer valid, and should not be relied upon by any system user. http://en.wikipedia.org/wiki/Certificate_revocation_list

Term	Acronym	Definition
Chief Information Officer	**CIO**	Job title for a manager responsible for Information Technology (IT) within an organization; often reports to the chief executive officer or chief financial officer. For information on the ASD/ Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) DoD CIO see DoDD 5144.1 of 2 May 2005. http://en.wikipedia.org/wiki/Chief_Information_Officer
Cipher Text	**CT**	Data that has been encrypted. Cipher text is unreadable until it has been converted into Plain Text (PT) (decrypted) with a key. http://www.webopedia.com/TERM/C/cipher_text.html
Collaboration		Allows users to work together securely on the network by way of video, audio, text chat, white boarding, online meetings, work groups, application sharing.
Collaboration Management Office	**CMO**	DISA organization responsible for fielding, sustaining and managing the life cycle of the Defense Collaboration Tool Suite (DCTS)
Commercial Off-The-Shelf	**COTS**	Products which are ready-made and available for sale to the general public. http://en.wikipedia.org/wiki/COTS
Common Access Card	**CAC**	A DoD-wide smart card used as the identification card for active duty Uniformed Services personnel (to include the Selected Reserve), DoD civilian employees, eligible contractor personnel, and eligible foreign nationals; the primary platform for the Public Key Infrastructure (PKI) authentication token used to access DoD computer networks and systems in the unclassified environment and, where authorized by governing security directives, the classified environment; and the principal card enabling physical access to buildings, facilities, installations, and controlled spaces as described in DoD Directive 8190.3, "Smart Card Technology," 31 August 2002. DoDI 88520.2.3, 1 April 2004, Enclosure (2) Definitions, page 13

Term	Acronym	Definition
Common Object Request Broker Architecture	**CORBA**	CORBA "wraps" code written in another language into a bundle containing additional information on the capabilities of the code inside, and explaining how to call it. The resulting wrapped objects can then be called from other programs (or CORBA objects) over the network. The CORBA specification defines APIs, communication protocol, and object/service information models to enable heterogeneous applications written in various languages running on various platforms to interoperate. http://en.wikipedia.org/wiki/CORBA
Community of Interest	**COI**	A collection of people who exchange information using a common vocabulary in support of shared missions, business processes, and objectives. The community is made up of the users/operators who participate in the information exchange, the system builders who develop computer systems for these users, and the functional proponents who define requirements and acquire systems on behalf of the users.
Component		In the context of a NESI Node, a Component can be a system, an application, a service, or another Node.
Computer Network Defense	**CND**	Defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation, or destruction. http://www.dtic.mil/doctrine/jel/doddict/data/c/01182.html
Computer Network Defense Service Provider	**CNDSP**	Those organizations responsible for delivering protection, detection and response services to its users. CNDS providers must provide for the coordination service support of a CNDS/CA. CNDS is commonly provided by a Computer Emergency or Incident Response Team (CERT/CIRT) and may be associated with a Network Operations (NetOps) and Security Center (NOSC). DoD Directive O-8530.1, *Computer Network Defense (CND)*, 8 January 2001, Enclosure 2 Definitions, p. 12
Content Discovery Service	**CDS**	Net-Centric Enterprise Services (NCES) service that provided a Federated Search capability.

Term	Acronym	Definition
Core Enterprise Services	**CES**	Generic information services that apply to any COI, provide the basic ability to search the enterprise for desired information, and then establish a connection to the desired service. http://www.defenselink.mil/nii/org/cio/doc/GIG_ES_Core_Enterprise_Services_Strategy_V1-1a.pdf
Defense Acquisition University	**DAU**	Combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. http://www.disa.mil/main/about/missman.html
Defense Collaboration Tool Suite	**DCTS**	A flexible, integrated set of applications providing interoperable, synchronous and asynchronous collaboration capability to the DoD agencies, Combatant Commands and Military Services. http://www.disa.mil/main/prodsol/dcts.html
Defense Enterprise Computing Center	**DECC**	DISA's five Defense Enterprise Computing Centers (DECCs) and their detachments operate hardware and software encompassing a broad spectrum of computing, storage and communications technologies. http://www.disa.mil/main/about/csc.html
Defense Information Systems Agency	**DISA**	Combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD Components, under all conditions of peace and war. http://www.disa.mil/main/about/missman.html
Design Pattern		General repeatable solution to a commonly-occurring problem in software design. A design pattern isn't a finished design that can be transformed directly into code; it is a description or template for how to solve a problem that can be used in many different situations. http://en.wikipedia.org/wiki/Design_pattern_%28computer_science%29
Discovery		Search, locate or publish data (content), other capabilities (services), or users across the Global Information Grid (GIG).

Term	Acronym	Definition
Document Object Model	**DOM**	A description of how an HTML or XML document is represented in an object-oriented fashion; DOM provides an application programming interface to access and modify the content, structure and style of the document. http://en.wikipedia.org/wiki/Document_Object_Model
DoD Active Directory Interoperability Working Group	**DADIWG**	
DoD Architecture Framework	**DoDAF**	Defines a common approach for DoD architecture description, development, presentation, and integration for both warfighting operations and business processes [DoDAF v1.0 supersedes C4ISR Architecture Framework v2.0, 18 December 1997]. Office of the Secretary of Defense memo of 9 Feb 2004, "The Department of Defense Architecture Framework (DoDAF)"
DoD Discovery Metadata Specification	**DDMS**	The DoD Discovery Metadata Specification (DDMS) defines discovery metadata elements for resources posted to community and organizational shared spaces. (Source: http://metadata.dod.mil/mdr/irs/DDMS/)
DoD Web Services Profile		Provides specifications and implementation guidelines to maximize interoperability across DoD Web Service implementations.
Domain Name System [or Service or Server]	**DNS**	An Internet service that translates domain names into Internet Protocol (IP) addresses. http://www.webopedia.com/TERM/D/DNS.html
Dynamic Host Configuration Protocol	**DHCP**	A protocol for assigning dynamic Internet Protocol (IP) addresses to devices on a network; DHCP a device can have a different IP address every time it connects to the network. http://www.webopedia.com/TERM/D/DHCP.html
Electronic Data Interchange Personnel Identifier	**EDI-PI**	A unique number assigned to each recipient of a Common Access Card (CAC), which is issued by the United States Department of Defense through the Defense Enrollment Eligibility Reporting System (DEERS). http://en.wikipedia.org/wiki/Electronic_Data_Interchange_Personal_Identifier

Term	Acronym	Definition
Electron-Trapping Optical Memory	**eTOM**	A method of erasable optical storage. Information is written, or stored, by a low-power laser tuned to a specific frequency. The laser elevates the energy level of electrons to a trapped state. The data is read by a second laser that returns the elevated electrons to their ground state. http://www.webopedia.com/TERM/E/ETOM.html
End-to-End	**E2E**	The end-to-end principle is one of the central design principles of the Internet Protocol (IP) that is the basis of the Internet. It states that, whenever possible, communications protocol operations should be defined to occur at the end-points of a communications system. In any computer communication, there are n >= 2 end points, called "end systems" or "hosts". End-to-end security means that sensitive data is encrypted all the way from your device side application back to the enterprise. Rather than relying on transport-level security such as Secure Socket Layer (SSL), end-to-end security puts the power of strong encryption in your hands, all through a simple interface. This ends the so-called “air gap” where sensitive data was previously decrypted at the gateway during translation for wireless protocols into Internet protocols. End-to-end monitoring is the process of attempting to access a Web server or other Internet device from across the Internet, just as a real end user would, to verify that the server is accessible and functioning properly at all times. This approach can be used instead of, or as a complement to, local monitoring software run by the Web Administrator. http://en.wikipedia.org/wiki/End-to-end
Enterprise		An organization considered as an entity or system that includes interdependent resources (e.g., people, organizations, and technology) that must coordinate functions and share information in support of a common mission or a set of related missions. In the computer industry, the term is often used to describe any large organization that utilizes computers. An intranet, for example, is a good example of an enterprise computing system. http://www.webopedia.com/TERM/e/enterprise.html

Term	Acronym	Definition
Enterprise Management Services	**EMS**	Enterprise Management Services (EMS) which are often used internal to a node, using a variety of COTS tools, which are fundamental to execution of Service Level Agreements (SLAs).
Enterprise Service Management		Monitor/manage Global Information Grid (GIG) Enterprise Services against operational performance parameters to ensure reliability and availability of critical capabilities.
Enterprise Services		In the DoD Global Information Grid (GIG) context, a set of services which provide visibility, access and delivery of data, and information services across the DoD enterprise.
eXtensible Access Control Markup Language	**XACML**	A declarative access control policy language implemented in XML. http://en.wikipedia.org/wiki/XACML
Extensible Markup Language	**XML**	A World Wide Web Consortium (W3C)-recommended general-purpose markup language for creating special-purpose markup languages, capable of describing many different kinds of data. In other words: XML is a way of describing data and an XML file can contain the data too, as in a database. It is a simplified subset of Standard Generalized Markup Language (SGML). The primary purpose is to facilitate the sharing of data across different systems, particularly systems connected via the Internet. Languages based on XML (for example, Geography Markup Language (GML), RDF/XML, RSS, MathML, Physical Markup Language (PML), XHTML, SVG, MusicXML and cXML) are defined in a formal way, allowing programs to modify and validate documents in these languages without prior knowledge of their form. http://en.wikipedia.org/wiki/Xml
Extensible Stylesheet Language Transformations	**XSLT**	A language to express the transformation of XML documents into other XML documents. (Source: W3C Glossary)
Façade Design Pattern		An object that provides a simplified interface to a larger body of code, such as a class library. http://en.wikipedia.org/wiki/Facade_pattern

Term	Acronym	Definition
Federated Search		Implementation of a computer program that allows users to access multiple data sources with a single query string located within a single interface. http://en.wikipedia.org/wiki/Federated_search
Firewall		A piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy, analogous to the function of firewalls in building construction.
GIG Router Working Group	**GRWG**	
Global Information Grid	**GIG**	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. DoDD 8100.1, *Global Information Grid (GIG) Overarching Policy*, 19 September 2002
Global Positioning System	**GPS**	A satellite constellation that provides highly accurate position, velocity, and time navigation information to users. [JP 1-02] http://www.dtic.mil/doctrine/jel/doddict/data/g/02300.html
High Assurance Internet Protocol Encryption	**HAIPE**	DoD version of Internet Protocol (IP) security (IPsec) protocol. http://en.wikipedia.org/wiki/HAIPE
Horizontal Fusion	**HF**	Horizontal Fusion (HF) is a direct response to Secretary of Defense Donald H. Rumsfeld's vision of Force Transformation. It demonstrates the ability to use lightweight automation to replace system mass with superior access to information based on a coherent architecture for an arbitrary future. Horizontal Fusion acts as a catalyst by implementing and demonstrating technologies and techniques that significantly advance the process of information-sharing in a an evolving net-centric environment. http://horizontalfusion.dtic.mil/vision/
IA/Security		Authorizes and authenticates Global Information Grid (GIG) users to ensure the confidentiality and integrity of information and services.

Term	Acronym	Definition
Identity Management		Provides the methodology and functions for maintaining information on people, consumers, and service providers. Supports the validation of identity authentication credentials.
Information Assurance	**IA**	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. CNSS Instruction No. 4009, Revised May 2003, "National Information Assurance (IA) Glossary"
Information Assurance Support Environment	**IASE**	DoD IA Portal managed by DISA. http://iase.disa.mil/index2.html
Information Support Plan	**ISP**	Used by program authorities to document the IT and National Security Systems (NSS) needs, objectives, interface requirements for all non-ACAT and fielded programs. CJCSI 6212.01C, 20 Nov 2003, Glossary page GL-11
Information Technology	**IT**	Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. Information technology does not include any equipment that is acquired by a federal contractor incidental to a federal contract. CJCSI 6212.01D, 8 March 2006, Glossary page GL-11)

Term	Acronym	Definition
Information Technology Laboratory	**ITL**	The ITL at the National Institute of Standards and Technology (NIST) has the broad mission of supporting U.S. industry, government, and academia with measurements and standards that enable new computational methods for scientific inquiry, assure IT innovations for maintaining global leadership, and re-engineer complex societal systems and processes through insertion of advanced Information Technology (IT). http://www.itl.nist.gov/itl-what_itl_does.html
Intelligence Community	**IC**	A federation of executive branch agencies and organizations that conduct intelligence activities necessary for conduct of foreign relations and protection of national security. http://www.intelligence.gov/
Internet Protocol	**IP**	Data packets routed across network, not switched via dedicated circuits.
Internet Protocol Version 4	**IPv4**	Version 4 of the Internet Protocol (IP). It was the first version of the Internet Protocol to be widely deployed, and forms the basis for most of the current Internet (as of 2004). It is described in IETF RFC 791, which was first published in September, 1981. IPv4 uses 32-bit addresses, limiting it to 4,294,967,296 unique addresses, many of which are reserved for special purposes such as local networks or multicast addresses. This reduces the number of addresses that can be allocated as public Internet addresses. As the number of addresses available is consumed, an IPv4 address shortage appears to be inevitable in the long run. This limitation has helped stimulate the push towards Internet Protocol Version 6 (IPv6), which is currently in the early stages of deployment, and may eventually replace IPv4. http://en.wikipedia.org/wiki/IPv4

Term	Acronym	Definition
Internet Protocol Version 6	**IPv6**	Version 6 of the Internet Protocol (IP); it was initially called IP Next Generation (IPng) when it was picked as the winner in the IETF's IPng selection process. IPv6 is intended to replace the previous standard, Internet Protocol Version 4 (IPv4), which only supports up to about 4 billion (4×10^9) addresses. IPv6 supports up to about 3.4×10^{38} (340 undecillion) addresses. This is the equivalent of 4.3×10^{20} (430 quintillion) addresses per square inch (6.7×10^{17} (670 quadrillion) addresses/mm²) of the Earth's surface. It is expected that IPv4 will be supported until at least 2025, to allow time for bugs and system errors to be corrected. http://en.wikipedia.org/wiki/Ipv6
Intrusion Detection System	**IDS**	Inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. http://www.webopedia.com/TERM/i/intrusion_detection_system.html
Java 2 Platform, Enterprise Edition	**J2EE**	See the Java Platform, Enterprise Edition (Java EE) entry http://java.sun.com/javaee/index.jsp
Java Platform, Enterprise Edition	**Java EE**	Industry standard for developing portable, robust, scalable and secure server-side Java applications. Building on the solid foundation of Java SE, Java EE provides Web services, component model, management, and communications APIs that make it the industry standard for implementing enterprise class service-oriented architecture (SOA) and Web 2.0 applications. The name of the Java platform for the enterprise has been simplified. Formerly, the platform was known as Java 2 Platform, Enterprise Edition (J2EE), and specific versions had "dot numbers" such as J2EE 1.4. The "2" is dropped from the name, as well as the dot number. So the next version of the Java platform for the enterprise is Java Platform, Enterprise Edition 5 (Java EE 5). http://java.sun.com/javaee/index.jsp

Term	Acronym	Definition
Joint Capabilities Integration and Development System	**JCIDS**	Establishes procedures to support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council (JROC) in identifying, assessing and prioritizing joint military capability. CJCSI 3170.01E, 11 May 2005, "Joint Capabilities Integration and Development System"
Joint Directory Services Working Group	**JDSWG**	
Joint Enterprise Directory Services Working Group	**JEDIWG**	
Joint Interoperability Test Command	**JITC**	Independent operational test and evaluation/assessor of DISA and other DoD Command, Control, Communications, Computers and Intelligence (C4I) acquisitions. http://jitc.fhu.disa.mil/mission.htm
Joint Worldwide Intelligence Communications System	**JWICS**	The sensitive, compartmented information portion of the Defense Information Systems Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. http://www.dtic.mil/doctrine/jel/doddict/data/j/02941.html
Key Interface Profile	**KIP**	An operational functionality, systems functionality and technical specifications description of the Key Interface. The profile consists of refined Operational and Systems Views, interface control specifications, Technical View with SV-TV Bridge, and referenced procedures for KIP compliance. The key interface profile is the technical specification that governs access to the GIG. CJCSI 6212.01D, 8 March 2006, Glossary page GL-14
Legacy System		An existing computer system or application program which continues to be used because the user (typically an organization) does not want to replace or redesign it. http://en.wikipedia.org/wiki/Legacy_system

Term	Acronym	Definition
Lightweight Directory Access Protocol	**LDAP**	A networking protocol for querying and modifying directory services running over Transmission Control Protocol/Internet Protocol (TCP/IP); an LDAP directory usually follows the X.500 model. http://en.wikipedia.org/wiki/Ldap
Link-16		Tactical Data Information Link (TADIL) primarily designed for use by Command and Control (C2) and Air-to-Air assets; uses the Joint Tactical Data Link (TADIL-J) message format. http://aatc.aztucs.ang.af.mil/aatcinfo.htm
Machine-to-Machine Messaging		Provides reliable machine-to-machine message exchange across the enterprise.
Mediation		Translates, brokers, aggregates, fuses or integrates data into commonly understood formats.
Messaging		Distributed, machine-to-machine messaging for notifications and alerts.
Metadata Services		Provides access to Extensible Markup Language (XML) components, data elements, taxonomy galleries, and validation and generation tools for DOD software developers.
Multicast		The delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once and only create copies when the links to the destinations split. http://en.wikipedia.org/wiki/Multicast
MX Record		A Mail eXchange (MX) Record is a type of resource record in the Domain Name System (DNS) specifying how Internet e-mail should be routed; MX records point to the servers to send an e-mail to, and which ones it should be sent to first, by priority. http://en.wikipedia.org/wiki/MX_Record
National Institute of Standards and Technology	**NIST**	Non-regulatory federal agency within the U.S. Commerce Department's Technology Administration with a mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. http://www.nist.gov/public_affairs/general2.htm

Term	Acronym	Definition
National Security Agency	**NSA**	America's cryptologic organization; it coordinates, directs, and performs highly specialized activities to protect U.S. government information systems and produce foreign signals intelligence information. http://www.nsa.gov/about/index.cfm
National Security Systems	**NSS**	Any telecommunications or information system operated by the Department of Defense (DoD), the function, operation, or use of which involves 1) intelligence activities, 2) cryptologic activities related to national security, 3) the command and control of military forces, 4) equipment that is an integral part of a weapons system, or 5) criticality to the direct fulfillment of military or intelligence missions. Defense Acquisition Acronyms and Terms, Twelfth Edition, July 2005, page B108
Net-Centric Enterprise Services	**NCES**	The Net-Centric Enterprise Services (NCES) program provides enterprise-level Information Technology (IT) services and infrastructure components, also called Core Enterprise Services (CES), for the Department of Defense (DoD) Global Information Grid (GIG).
Net-Centric Implementation Directives	**NCIDs**	

Term	Acronym	Definition
Net-Centric Operations and Warfare Reference Model	**NCOW RM**	The NCOW RM describes the activities required to establish, use, operate, and manage the net-centric enterprise information environment to include: the generic userinterface, the intelligent-assistant capabilities, the net-centric service capabilities (core services, Community of Interest (COI) services, and environment control services), and the enterprise management components. It also describes a selected set of key standards that will be needed as the NCOW capabilities of the Global Information Grid (GIG) are realized. The NCOW RM represents the objective end-state for the GIG. This objective end-state is a service-oriented, inter-networked, information infrastructure in which users request and receive services that enable operational capabilities across the range of military operations; DOD business operations; and Department-wide enterprise management operations. The NCOW RM is a key compliance mechanism for evaluating DOD information technology capabilities and the Net-Ready Key Performance Parameter. CJCSI 6212.01D, 8 March 2006, Glossary pages GL-17 and GL-18
Net-Ready Key Performance Parameter	**NR-KPP**	Measures the net-centricity of a new program or major upgrade.
Network Intrusion Detection	**NID**	Attempt to detect malicious activity such as denial of service attacks, port-scans or even attempts to crack into computers by monitoring network traffic. http://en.wikipedia.org/wiki/Network_intrusion-detection_system

Term	Acronym	Definition
Network Operations	**NetOps**	An organizational, procedural, and technological construct for ensuring information and decision superiority at the strategic, operational, and tactical levels of warfare as well as within DOD business operations. NetOps is an operational approach, which addresses the interdependency and integration of IA/CND, S&NM, and CS capabilities. NetOps consists of the organizations, tactics, techniques, procedures, functionalities, and technologies required to plan, administer, and monitor use of the Global Information Grid (GIG) infrastructure and the end-to-end information flows of the GIG; and to respond to threats, outages, and other operational impact. NetOps ensures mission requirements are properly considered in GIG operational decision-making. NetOps enables the GIG to provide its users with information they need, when they need it, where they need it, with appropriate protection of the information. NetOps is an essential capability for successful execution of net-centric warfare and other net-centric operations in support of national security objectives. http://en.wikipedia.org/wiki/Netops
Network Time Protocol	**NTP**	Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. NTP uses User Datagram Protocol (UDP) port 123 as its transport layer. It is designed particularly to resist the effects of variable latency. http://en.wikipedia.org/wiki/Network_Time_Protocol
Networks and Information Integration	**NII**	See Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) entry; acronym also expands to National Information Infrastructure
New Generation Operations Support Systems	**NGOSS**	TeleManagement Forum (TMF) term for its description of the optimum way for a Communications Service Provider (CSP) to manage its business. It describes how to integrate Operational Support Systems (OSS) and provides technical deliverables to assist with this integration. http://en.wikipedia.org/wiki/NGOSS
Next Generation Collaboration Service	**NGCS**	DISA pilot for Services, Combatant Commands (COCOMs), and Defense agencies which concluded on 2 September 2005. http://www.disa.mil/ges.ngcs.html

Term	Acronym	Definition
Node		In general network usage, a node is a processing location such as a computer or some other device. Every node has a unique network address, sometimes called a Data Link Control (DLC) address or Media Access Control (MAC) address. http://www.webopedia.com/TERM/n/node.html A NESI Node is a collection of integrated components (i.e., systems, applications, services and other Nodes) that are bound together spatially and/or temporally to meet the needs of a particular mission. It is conceptual in nature and can not be defined in terms of a concrete set of components or size. The membership of a component within a particular Node is not exclusive and a Component can be part of multiple Nodes.
Non-secure Internet Protocol Router Network	**NIPRNET**	Provides seamless interoperability for unclassified combat support applications, as well as controlled access to the Internet. Direct connection data rates range from 56Kbps to 155Mbps. Remote dial-up services are available up to 56Kbps. http://www.disa.mil/main/prodsol/data.html
Online Certificate Status Protocol	**OCSP**	Internet Protocol (IP) used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a Public Key Infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed *OCSP responders*. http://en.wikipedia.org/wiki/Ocsp

Term	Acronym	Definition
Operational View	**OV**	The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions. DoD missions include both warfighting missions and business processes. The OV contains graphical and textual products that comprise an identification of the operational nodes and elements, assigned tasks and activities, and information flows required between nodes. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges. DoDAF Volume I, 9 February 2004, Section 1.3.1, page 1-2
Orchestration		Co-ordination of events in a process; orchestration directs and manages the on-demand assembly of multiple component services to create a composite application or business process. http://looselycoupled.com/glossary/orchestration
Organization for the Advancement of Structured Information Standards	**OASIS**	A not-for-profit, international consortium that drives the development, convergence, and adoption of e-business standards. http://www.oasis-open.org/who/
Plain Text	**PT**	Refers to textual data in ASCII format. Plain text is the most portable format because it is supported by nearly every application on every machine. It is quite limited, however, because it cannot contain any formatting commands. In cryptography, plain text refers to any message that is not encrypted. http://www.webopedia.com/TERM/p/plain_text.html
Platform		In computing, a platform describes some sort of framework, either in hardware or software, which allows software to run. Typical platforms include a computer's architecture, operating system, or programming languages and their runtime libraries. http://en.wikipedia.org/wiki/Platform_%28computing%29
Plug-in		A hardware or software module that adds a specific feature or service to a larger system. http://www.webopedia.com/TERM/p/plug_in.html

Term	Acronym	Definition
Portlet		A reusable Web component that displays relevant information to portal users. Examples for portlets include email, weather, discussion forums, and news. The purpose of the Web Services for Remote Portlets (WSRP) interface is to provide a Web services standard that allows for the "plug-n-play" of portals, other intermediary Web applications that aggregate content, and applications from disparate sources. The portlet specification enables interoperability between portlets and portals. This specification defines a set of APIs for portal computing that addresses the areas of aggregation, personalization, presentation, and security. http://en.wikipedia.org/wiki/Portlets
Protocol		An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, data compression method, if any, how the sending device will indicate that it has finished sending a message, and how the receiving device will indicate that it has received a message. http://www.webopedia.com/TERM/p/protocol.html
Proxy		A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server. Proxy servers have two main purposes: improve performance and filter requests. http://www.webopedia.com/TERM/p/proxy_server.html
Public Key		Public key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key. http://en.wikipedia.org/wiki/Public_key; 17 April 2007

Term	Acronym	Definition
Public Key Infrastructure	**PKI**	Framework established to issue, maintain, and revoke public key certificates accommodating a variety of security technologies, including the use of software. CNSS Instruction No. 4009, Revised May 2003, "National Information Assurance (IA) Glossary"
Quality of Service	**QoS**	Networking term that specifies a guaranteed throughput level. http://www.webopedia.com/TERM/Q/QoS.html
Registration Web Service	**RWS**	Horizontal Fusion (HF) service used by data producers to register content sources.
Request for Quotation	**RFQ**	A solicitation used in negotiated acquisition to communicate government requirements to prospective contractors and to solicit a quotation. A response to an RFQ is not an offer; however, it is informational in character. Defense Acquisition Acronyms and Terms, Twelfth Edition, July 2005, page B-140
Router		A device that forwards data packets along networks. A router is connected to at least two networks, commonly two local area networks (LANs) or wide area networks (WANs) or a LAN and its Internet Service Provider's network. Routers are located at gateways, the places where two or more networks connect. http://www.webopedia.com/TERM/r/router.html
Schema		The structure of a database system, described in a formal language supported by the database management system (DBMS). http://www.webopedia.com/TERM/s/schema.html
Search Web Service	**SWS**	Horizontal Fusion (HF) service used to search for content from registered sources.

Term	Acronym	Definition
SECRET Internet Protocol Router Network	**SIPRNET**	DoD's largest interoperable command and control data network, supporting the Global Command and Control System (GCCS), the Defense Message System (DMS), collaborative planning and numerous other classified warfighter applications. Direct connection data rates range from 56 kbps to 155 Mbps for the Non-secure Internet Protocol Router Network (NIPRNET), and up to 45 Mbps for the SIPRNET. Remote dial-up services are also available, ranging from 19.2 kbps on SIPRNET to 56 kbps on NIPRNET. http://www.disa.mil/main/prodsol/data.html
Secure Socket[s] Layer	**SSL**	A technology that allows Web browsers and Web servers to communicate over a secured connection. The protocol runs above Transmission Control Protocol/Internet Protocol (TCP/IP) and below application protocols. http://java.sun.com/j2ee/1.4/docs/glossary.html
Security Assertion Markup Language	**SAML**	An XML standard for exchanging authentication and authorization data between security domains; that is, between an identity provider and a service provider. SAML is a product of the Organization for the Advancement of Structured Information Standards (OASIS) Security Services Technical Committee. http://en.wikipedia.org/wiki/SAML
Security Technical Implementation Guide	**STIG**	Configuration standards for DOD IA and IA-enabled devices/systems. http://iase.disa.mil/stigs/index.html
Sensitive Compartmented Information	**SCI**	Classified information concerning or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of Central Intelligence (DCI). DoDD 8520.1, 20 December 2001, Subject: Protection of Sensitive Compartmented Information (SCI), Page 2, Section 3.3
Server		A computer or device on a network that manages network resources. http://www.webopedia.com/TERM/s/server.html

Term	Acronym	Definition
Service		A service is any function that has a clearly defined interface accessed through well-defined public access points.
Service Definition Framework	**SDF**	SDF provides service users, customers, developers, providers, and managers with a common frame of reference. Its structure and methodology enable you to fully define the Service Access Points (SAPs) for the service.
Service Discovery	**SD**	Provides a "yellow pages," categorized by DOD function, enabling users to advertise and locate capabilities available on the network.
Service Level Agreement	**SLA**	A contract between an Application Service Provider (ASP) and the end user which stipulates and commits the ASP to a required level of service. An SLA should contain a specified level of service, support options, enforcement or penalty provisions for services not provided, a guaranteed level of system performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be provided and for what fee. http://www.webopedia.com/TERM/S/Service_Level_Agreement.html
Service Management		Enables monitoring of DOD Web services. Provides reporting of service-level information to potential and current service consumers, program analysts, and program managers.
Service Mediation		Allows disparate applications to work together across the enterprise by supporting the transformation of information from one format to another, and the correlation and fusion of data from diverse sources. Supports creation and implementation of process workflows across the enterprise.
Service Security		Provides a layer of Defense in Depth that enables protection, defense, and integrity of the information environment.

Term	Acronym	Definition
Simple Object Access Protocol	**SOAP**	A lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet Protocols (IPs), including SMTP, MIME, and HTTP. http://www.webopedia.com/TERM/S/SOAP.html
Situation Awareness Data Link	**SADL**	An Enhanced Position Location and Reporting System (EPLRS) radio modified for use in an aircraft. SADL and EPLRS radios are used to establish a common secure tactical data link network. http://aatc.aztucs.ang.af.mil/aatcinfo.htm
Smart Card		A credit card-size device, normally for carrying and use by personnel, that contains one or more integrated circuits and also may employ one or more of the following technologies: magnetic stripe, bar codes (linear and two-dimensional), non-contact and radio frequency transmitters, biometric information, encryption and authentication, or photo identification. DoDD 8190.3, *Smart Card Technology*, 31 August 2003, Page 2, Section 3.2
Software Development Kit	**SDK**	A programming package that enables a programmer to develop applications for a specific platform; typically, an SDK includes one or more APIs, programming tools, and documentation. http://www.webopedia.com/TERM/S/SDK.html
Software Product Line	**SPL**	A software product line (SPL) is a set of software-intensive systems that share a common, managed set of features satisfying the specific needs of a particular market segment or mission and that are developed from a common set of core assets in a prescribed way. Software Engineering Institute
Spyware		Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. http://www.webopedia.com/TERM/s/spyware.html
Stakeholder		Person or organization that has a legitimate interest in a project or entity. http://en.wikipedia.org/wiki/Stakeholder

Term	Acronym	Definition
Storage		Provides physical and virtual places to host and retain data for purposes such as content staging, continuity of operations, or archival.
Sustainment		One of the two major efforts (with disposal) of the Operations and support phase of a DoD acquisition program. Sustainment includes supply, maintenance, transportation, sustaining engineering, data management, configuration management, manpower, personnel, training, habitability, survivability, environment, safety (including explosives safety), occupational health, protection of critical program information, anti-tamper provisions, and Information Technology (IT), including National Security Systems (NSS), supportability and interoperability functions. DoDI 5000.2, 12 May 2003, "Operation of the Defense Acquisition System"
System		Two or more interrelated pieces of equipment (or sets) arranged in a package to perform an operational function or to satisfy a requirement. Defense Acquisition Glossary of Terms, Jan 2001
Systems View	**SV**	A set of graphical and textual products that describes systems and interconnections providing for, or supporting, DoD functions. DoD functions include both warfighting and business functions. The SV associates systems resources to the Operational View (OV). These systems resources support the operational activities and facilitate the exchange of information among operational nodes. DoDAF v1 Vol. 1, 9 Feb 2004, pages 1-2 and 1-3, section 1.3.2

Term	Acronym	Definition
Technical Standards View	**TV**	The minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The TV includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture. DoDAF v1 Vol. 1, 9 Feb 2004, page 1-3, section 1.3.3
Transmission Control Protocol	**TCP**	One of the core protocols of the Internet Protocol (IP) suite. Using TCP, programs on networked computers can create connections to one another, over which they can send data. The protocol guarantees that data sent by one endpoint will be received in the same order by the other, without any pieces missing. It also distinguishes data for different applications (such as a Web server and an email server) on the same computer. http://en.wikipedia.org/wiki/Transmission_Control_Protocol
Transmission Control Protocol/Internet Protocol	**TCP/IP**	A suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP. TCP/IP is built into the UNIX operating system and is used by the Internet, making it the de facto standard for transmitting data over networks. Even network operating systems that have their own protocols, such as Netware, also support TCP/IP.
Transport Level Security	**TLS**	A protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet. http://www.webopedia.com/TERM/T/TLS.html
Trust Point		A trust point is a Certificate Authority (CA) that is the root of all trust for all CAs in a CA hierarchy.

Term	Acronym	Definition
Trusted Guard		Accredited to pass information between two networks at different security levels according to well defined rules and other controls. Guard products only pass defined types of information (e.g., email, images, or formatted messages). A key challenge is how to implement net-centric operations across trusted guards in the presence of CES services.
Universal Description, Discovery, and Integration	**UDDI**	An industry initiative to create a platform-independent, open framework for describing services, discovering businesses, and integrating business services using the Internet, as well as a registry. It is being developed by a vendor consortium. http://java.sun.com/j2ee/1.4/docs/glossary.html
Universal Naming Convention	**UNC**	Specifies a common syntax for accessing network resources, such as shared folders and printers. http://en.wikipedia.org/wiki/Universal_Naming_Convention
User Assistance		Provides automated "helper" capabilities and user preferences to help maximize user efficiency in task performance.
User Datagram Protocol	**UDP**	A connectionless protocol that, like TCP, runs on top of Internet Protocol (IP) networks. Unlike Transmission Control Protocol/Internet Protocol (TCP/IP), UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It's used primarily for broadcasting messages over a network. http://www.webopedia.com/TERM/U/User_Datagram_Protocol.html
Virtual Private Network	**VPN**	A network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable the creation of networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. http://www.webopedia.com/TERM/V/VPN.html
Web Archive	**WAR**	A ZIP file used to distribute a set of Java classes. http://en.wikipedia.org/wiki/WAR_%28file_format%29

Term	Acronym	Definition
Web Service		A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP-messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards. (Source: http://www.w3.org/TR/ws-gloss/)
Web Services Atomic Transaction	**WS-AtomicTransaction**	This specification provides the definition of the atomic transaction coordination type that is to be used with the extensible coordination framework described in the WS-Coordination specification. The specification defines three specific agreement coordination protocols for the atomic transaction coordination type: completion, volatile two-phase commit, and durable two-phase commit. Developers can use any or all of these protocols when building applications that require consistent agreement on the outcome of short-lived distributed activities that have the all-or-nothing property. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/
Web Services Business Activity	**WS-BusinessActivity**	This specification provides the definition of the business activity coordination type that is to be used with the extensible coordination framework described in the WS-Coordination specification. The specification defines two specific agreement coordination protocols for the business activity coordination type: BusinessAgreementWithParticipantCompletion and BusinessAgreementWithCoordinatorCompletion. Developers can use any or all of these protocols when building applications that require consistent agreement on the outcome of long-running distributed activities. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/

Term	Acronym	Definition
Web Services Coordination	**WS-Coordination**	This specification describes an extensible framework for providing protocols that coordinate the actions of distributed applications. Such coordination protocols are used to support a number of applications, including those that need to reach consistent agreement on the outcome of distributed activities. The framework defined in this specification enables an application service to create a context needed to propagate an activity to other services and to register for coordination protocols. The framework enables existing transaction processing, workflow, and other systems for coordination to hide their proprietary protocols and to operate in a heterogeneous environment. Additionally this specification describes a definition of the structure of context and the requirements for propagating context between cooperating services. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/
Web Services Description Language	**WSDL**	An XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocols and message format to define an endpoint.
Web Services for Remote Portlets	**WSRP**	The WSRP specification defines a Web service interface for interacting with interactive presentation-oriented Web services. It has been produced through the joint efforts of the Web Services for Interactive Applications (WSIA) and Web Services for Remote Portals (WSRP) OASIS Technical Committees. Scenarios that motivate WSRP/WSIA functionality include (1) portal servers providing portlets as presentation-oriented Web services that can be used by aggregation engines; (2) portal servers consuming presentation-oriented Web services provided by portal or non-portal content providers and integrating them into a portal framework. (Source: http://www.oasis-open.org/committees/download.php/3343/oasis-200304-wsrp-specification-1.0.pdf)

Term	Acronym	Definition
Web Services Interoperability Organization	**WS-I**	WS-I is an open industry organization chartered to promote Web services interoperability across platforms, operating systems and programming languages. http://www.ws-i.org/
Web Services Transaction	**WS-Transaction**	A set of specifications (WS-Coordination, WS-AtomicTransaction, and WS-BusinessActivity) that define mechanisms for transactional interoperability between Web services domains and provide a means to compose transactional qualities of service into Web services applications. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-tx/
World Wide Web Consortium	**W3C**	The World Wide Web Consortium (W3C) is an international consortium where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure long-term growth for the Web. http://www.w3.org/Consortium/

Guidance Details

G1569

Statement:	Maintain a comprehensive list of all of the Components that are part of the Node.
Rationale:	Throughout the lifecycle of a Node (from design to instantiation), this action is fundamental to the provisioning of a shared infrastructure and the avoidance of functional duplication within the Node. This activity has a direct impact on the design and implementation requirements during acquisition.
Derived From	
Justifies	
Referenced By	Nodes as Stakeholders
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1.** **Test:** *Is there a list of Components that comprise the Node?* **Procedure:** Examine the documents (for example, the Node's design requirements) and look for a list of Components. **Examples:** None.

G1570

Statement:	Assume an active management role among the Components within the Node.
Rationale:	Involvement of the Node as a stakeholder in its Components (from design to instantiation) has a bearing on Global Information Grid (GIG) interoperability. Strong coordination among a Node's Components will likely avoid the external exposure of inconsistencies or, worse, incomplete, inaccurate, or misunderstood data.
Derived From	
Justifies	

Referenced By	Nodes as Stakeholders
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do the Components of the Node list the Node as a primary stakeholder in their [appropriate acquisition document]?* **Procedure:** Check the [appropriate acquisition document] of the Components and determine if the Node is listed as a stakeholder or if there are requirements for coordinating with the Node. **Examples:** A Component's CDD may state a requirement for participating in a Node which could satisfy this requirement. **2. Test:** Do the Components of the Node set forth requirements in their [appropriate acquisition document] for coordinating with the Node. **Procedure:** Check the [appropriate acquisition document] of the Components and determine if the Node is listed as a stakeholder or if there are requirements for coordinating with the Node. **Examples:** A Component's CDD may state a requirement for participating in a Node which could satisfy this requirement.

G1571

Statement:	Maintain a comprehensive list of all the Communities of Interest (COIs) to which the Components of a Node belong.
Rationale:	The Node infrastructure must be engineered to support the information exchange between Communities of Interests (COIs). If a comprehensive list of COIs is not created and maintained then the infrastructure may no longer be adequate and may continue to make provisions for COIs that are no longer a part of the Node.
Derived From	
Justifies	

Referenced By	Net-Centric Information Engineering
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do the Node's Components have representation registered within the DoD Metadata Registry as members of the Communities of Interest (COIs)?* **Procedure:** Examine the DoD Metadata Registry for members of the Node organization that are members of the pertinent COIs. **Examples:** None.

G1572

Statement:	Include the Node as a party to any Service Level Agreements (SLAs) signed by any of the Components of the Node.
Rationale:	The Node has a stake in performance specifications provided in the Service Level Agreements (SLA). Since the SLA is a contract that commits the application service provider to a required level of service. The Node must be able to support that level of service with its infrastructure.
Derived From	
Justifies	
Referenced By	Net-Centric Information Engineering
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node have copies of all Service Level Agreements (SLAs) signed by its Components?* **Procedure:** Compare the Service Level Agreements (SLAs) against the service Components supported by the Node. **Examples:** None.

G1573

Statement:	Define the enterprise design patterns that a Node supports.
Rationale:	The Node infrastructure must be engineered to support information exchanges between various COIs. The COIs can require any number of Components to fulfill the COIs mission, When a Component wishes to make its data available over the enterprise, there are different enterprise design pattern which can be used. For example, the mechanism selected by a Component to exchange information may be publish-subscribe, broker, or client server. The Node infrastructure must support whichever enterprise design pattern mechanism is selected.
Derived From	
Justifies	
Referenced By	Net-Centric Information Engineering
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node document which types of enterprise design patterns it supports?* **Procedure:** Look through the Node documents for a list of enterprise design patterns it supports. **Examples:** None.

G1574

Statement:	Define which enterprise design patterns a Component requires.
Rationale:	A Component should document which enterprise design patterns it intends to capitalize on to meet its mission. For example, a client interested in using a client-server weather service, could have problems if the weather service is a real-time publish-subscribe service. This action clarifies for the Node which enterprise design patterns are required by its Components and provides direction for which patterns to support at the Node level.
Derived From	

Justifies	
Referenced By	Net-Centric Information Engineering
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Component indicate which type of enterprise design pattern it will use?* **Procedure:** Look through the Component documentation and that defines what type of enterprise design pattern it uses. **Examples:** None.

G1575

Statement:	Designate Node representatives to relevant Communities of Interest (COIs) in which Components of the Node participate.
Rationale:	"COIs is the inclusive term used to describe collaborative groups of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange." The principal mechanism for recording COI agreements is the DoD Metadata Registry required by the DoD CIO Memorandum "DoD Net-Centric Data Management Strategy: Metadata Registration." There are registry implementations on the Non-secure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET), and Joint Worldwide Intelligence Communications System (JWICS).
Derived From	
Justifies	
Referenced By	Net-Centric Information Engineering
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node have representation registered within the Metadata Registry as members of the Communities of Interest (COIs)?*

	Procedure: Examine the DoD Metadata Registry for members of the Node organization that are members of the pertinent COIs. **Examples:** None.

G1576

Statement:	Provide an environment to support the development, build, integration, and test of net-centric capabilities.
Rationale:	Nodes should provide an environment to support the development, integration, and testing of net-centric capabilities of its Components. As Nodes themselves and the Components within the Nodes move closer to the implementation of net-centric capabilities, it becomes increasingly important to provide a development, integration, and test environment to support those capabilities. This environment should allow for the exercise not just the Node infrastructure, but also either host locally within the Node, or provide access to, Net-Centric Enterprise Services (NCES) piloted services. The particulars on how this is done depend on the characteristics of the Node. For example, mobile or deployed Nodes would provide environments substantially different than fixed land-based or permanent Nodes.
Derived From	
Justifies	
Referenced By	Internal Component Environment, CES Definitions and Status
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Are there instructions on how to develop, build, integrate or test Components within the Node?* **Procedure:** Look for user guides or installation instructions that cover the Node environment. **Examples:** None.

G1577

Statement:	Maintain an enterprise service schedule for interim and final enterprise

	capabilities within the Node.
Rationale:	The current state of Enterprise Services is in flux. Developing Components that rely on those services can create a circular problem for development. An enterprise service schedule for interim and final capabilities will help elevate the co-dependencies of the Component lifecycle from the Node lifecycle.
Derived From	
Justifies	
Referenced By	Internal Component Environment, Orchestration of Node and Enterprise Services, CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Is there an enterprise service schedule or roadmap that covers interim and final capabilities of the Node?* **Procedure:** Look for the existence of the schedule or a roadmap for the Node. **Examples:** None.

G1578

Statement:	Define a schedule for Components that includes the use of the Enterprise Services defined within the Node's Enterprise Service schedule.
Rationale:	The exercise of matching those Enterprise Services required by the Component to those provided by the Node can help identify and gaps in the Node's functionality. By tying the Component's enterprise services to the Node's enterprise schedule, critical paths may be identified in the Node's schedule.
Derived From	
Justifies	
Referenced By	Internal Component Environment, Orchestration of Node and Enterprise Services, CES Parallel Development

Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Component have an enterprise service schedule or roadmap that shows the progression of enterprise service usage by interim and final capabilities of the Component?* **Procedure:** Look for the existence of the schedule or a roadmap for the Component. **Examples:** None.

G1579

Statement:	Define which Enterprise Services the Node will host locally when the Node becomes operational.
Rationale:	Locally defined Enterprise Services are inherently faster and less susceptible to network failures and traffic than local services. If a Component requires performance based or critical enterprise services that the Node will only provide as a proxy, then development, building, integration and testing should be done to the local enterprise service specification. If the Node developed enterprise service will not be ready until near the end of the Component's schedule, take steps to minimize risk.
Derived From	
Justifies	
Referenced By	Internal Component Environment
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node specification identify which Enterprise Services will be locally defined within the Node?* **Procedure:** Review the Node specification for a list of Enterprise Services that will be locally defined within the Node. **Examples:** None.

G1580

Statement:	Define which Enterprise Services will be hosted over the Global Information Grid (GIG) when the Node becomes operational.
Rationale:	Enterprise Services that are defined using proxies should have interfaces that follow the standards defined by the enterprise service provider. Therefore, the access to the server should be fairly stable and almost static in nature with few changes. These are services that should be in the critical path of a Component's mission.
Derived From	
Justifies	
Referenced By	Internal Component Environment
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node specification identify which Enterprise Services will be defined using proxies?* **Procedure:** Review the Node specification for a list of Enterprise Services that will be defined using proxies. **Examples:** None.

G1581

Statement:	Expose legacy system or application functionality through the use of a service that uses a façade design pattern.
Rationale:	Nodes might contain systems or applications that are in the Sustainment lifecycle phase. These Components are often referred to as "legacy" systems or applications. If a Node needs to expose functionality or data form the legacy Component, changing the internals of such Components to support net-centricity is often impractical with little return on investment. This design pattern offers a reasonable interim solution.
Derived From	
Justifies	

Referenced By	Integration of Legacy Systems
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node use façade design patterns such as the wrapper or adapter pattern to expose the functionality of legacy systems or applications?* **Procedure:** Make sure that all the Components that are exposed to the internal Node Components or to the external network (with the Node as a proxy) use a façade design pattern such as wrapper or adapter. **Examples:** None.

G1582

Statement:	In Nodal Enterprise Services schedules, include version numbers of standard Enterprise Services interfaces being implemented.
Rationale:	Given the complexity, varied implementation timing, and leading edge nature of Enterprise Services, the orchestration of efforts is essential for the successful integration of the Node's Components. The dependencies captured by such a schedule should clearly show what capabilities will be available and when during the Node's lifecycle.
Derived From	
Justifies	
Referenced By	Orchestration of Node and External Enterprise
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Are Enterprise Services interface versions provided on the enterprise service schedule for the Node?* **Procedure:** Review the Enterprise Services schedule published for the Node and make sure the schedule provides necessary details including specific version numbers, workarounds, assumptions, constraints and configuration

	limitations that are interwoven into the schedule. **Examples:** An Enterprise Service might be releasing a new version during the lifecycle of the Node's development; which version's functionality will be available when is essential for the successful integration of the Node's Components. **2. Test:** *Are Enterprise Services interface versions provided on the enterprise service schedule for the Component?* **Procedure:** Review the Enterprise Services schedule published for the Component and make sure the schedule provides necessary details including specific version numbers, workarounds, assumptions, constraints and configuration limitations that are interwoven into the schedule. **Examples:** An Enterprise Service might be releasing a new version during the lifecycle of the Node's development; which version's functionality will be available when is essential so the Component can utilize the appropriate available capabilities.

G1583

Statement:	Provide routine Enterprise Services schedule updates to every Component of a Node.
Rationale:	A fundamental justification for the existence of nodes is to ensure it provides a shared infrastructure for its Components. If that infrastructure evolves independently of the Components, then they may be developed at timeframes and rates of evolution that differ from the capabilities of the available shared infrastructure. In addition, Components may be members of multiple Nodes, providing an additional coordination challenge. Regular updates to the Componetns of the master schedule will assist in managing this challenge.
Derived From	
Justifies	
Referenced By	Orchestration of Internal Components

Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Are there multiple iterations of the Enterprise Services schedule developed over time and is the most recent update timely?* **Procedure:** Check for version numbering and release dates of the Enterprise Services schedule. Ensure that a reasonably recent update is available. **Examples:** None.

G1584

Statement:	Provide a transport infrastructure that is shared among Components within the Node.
Rationale:	Transport elements provided by the Node are a means for the Node to implement GIG IA boundary protections, bind Components together, and satisfy other enterprise requirements. As transport elements are an essential piece of the net-centric puzzle, they also play a key role in minimizing interoperability issues. A Node's provisioning of the shared transport and related guidance is a key aspect of its existence.
Derived From	
Justifies	
Referenced By	Node Transport
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node's design provide for a transport infrastructure?* **Procedure:** Review the Node's infrastructure design and ensure that the Node provides the necessary transport elements for shared use by its Components. **Examples:** None. **2. Test:** *Are the Node's Components using the Node provisioned transport infrastructure?*

	Procedure:	Review the design of the Node's Components (see [G1569]) and ensure that they all utilize the common transport infrastructure of inter-Nodal communication.
	Examples:	None.

G1585

Statement:	Provide a transport infrastructure for the Node that implements Global Information Grid (GIG) Information Assurance (IA) boundary protections.
Rationale:	The Global Information Grid (GIG) is intended to be the "outside world" for all the Components within the Node. In order to protect the Components within the Node from the "outside world" and to protect the "outside world" from the Node, the Node should control the IA Boundary.
Derived From	
Justifies	
Referenced By	Node Transport
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Is there an IA device in the acquisition list?* **Procedure:** Look for an IA device within the parts list for the Node. **Examples:** **2. Test:** *Is the IA device configured to meet security requirements?* **Procedure:** Check the Node's IA installation guide and look for procedures that describe how to configure the IA device for the Nodes particular needs. **Examples:** None.

G1586

Statement:	Provide a transport infrastructure for the Node that is Internet Protocol Version 6 (IPv6) capable in accordance with the appropriate governing transition plan.
Rationale:	During the transition period in the DoD community (FY06-FY15) networks, services and applications will be in a mixed environment. All Critical KPPs must be able to operate in an Internet Protocol Version 4 (IPv4) only network, an Internet Protocol Version 6 (IPv6) only network, and a dual-stack network. See Section 4.1, DoD IPv6 Standard Profiles for IPv6 Capable Products.
Derived From	
Justifies	
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the system operate in an Internet Protocol Version 6 (IPv6) only Network?* **Procedure:** Critical Functions will be tested in a Network that only supports Internet Protocol Version 6 (IPv6). The host must be able to complete all critical functions utilizing only IPv6 on the network (no tunneling). **Examples:** None.

G1587

Statement:	Prepare an Internet Protocol Version 6 (IPv6) transition plan for the Node.
Rationale:	The transition from Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6) is non-trivial and requires a great deal of coordination and effort on the part of everyone involved. The transition plan helps to minimize the potential disastrous side effects of the transition.
Derived From	

Justifies	
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Is there an Internet Protocol Version 6 (IPv6) transition plan for the Node?* **Procedure:** Look for an Internet Protocol Version 6 (IPv6) transition plan document. **Examples:** None.

G1588

Statement:	Coordinate an Internet Protocol Version 6 (IPv6) transition plan for a Node with the Components that comprise the Node.
Rationale:	The effects of the transition from Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6) is isolated in the Node infrastructure put can have impacts on all the Components that comprise the Node. The transition Plan should cover a "window" that allows all the Components to operate in either IPv4 or IPv6 (i.e., Dual Stack Mode) to make the transition.
Derived From	
Justifies	
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Does the plan allow for a "Dual Stack" environment at least during some transition period?* **Procedure:** Look for a part of the transition plan that addresses "Dual Stack" mode of operation. **Examples:** None.

G1589

Statement:	Address issues in the appropriate governing IPv6 transition plan as part of the Internet Protocol Version 6 (IPv6) Transition Plan for a Node.
Rationale:	DoD has mandated each service create an IPv6 transformation office to manage the transition to IPv6. Node transition plans must be aligned and in conformance with the appropriate governing office's plans or criteria.
Derived From	
Justifies	
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Does the Node's IPv6 Transition Plan have a section that addresses specific criteria established by the appropriate governing IPv6 transition office or plan?* **Procedure:** Review the IPv6 plan for a section or specific criteria that address the appropriate items from the appropriate governing plan or is approved by the appropriate governing office. **Examples:** The Air Force IPv6 Transition Office requires each program to develop a plan with approval by the transition office (in lieu of aligning with a central plan). To check an Air Force Node's alignment, look to see that the Node's IPv6 transition plan is approved by the appropriate authority.

G1590

Statement:	Include transition of all the impacted elements of the network as part of the Internet Protocol Version 6 (IPv6) Transition Plan for a Node.
Rationale:	Internet Protocol Version 6 (IPv6) transition has an impact on many transport infrastructure Components. The Node's IPv6 Transition Plan should include transition of all impacted network elements including

	DNS, routing, security, and dynamic address assignment. The DoD IPv6 Network Engineer's Guidebook (Draft) and the DoD IPv6 Application Engineer's Guidebook (Draft) provide guidance for transition of impacted Components.
Derived From	
Justifies	G1599, G1600, BP1705
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the transition to IPv6 on the Domain Name Service (DNS)?* **Procedure:** Review the plan and look for a section dedicated to the Domain Name Service (DNS). At a minimum, it should indicate that there is no impact. **Examples:** None. **2. Test:** *Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the transition to IPv6 on routing?* **Procedure:** Review the plan and look for a section dedicated to routing. At a minimum, it should indicate that there is no impact. **Examples:** None. **3. Test:** *Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the transition to IPv6 on security?* **Procedure:** Review the plan and look for a section dedicated to security. At a minimum, it should indicate that there is no impact. **Examples:** None. **4. Test:** *Does the Internet Protocol Version 6 (IPv6) Transition Plan address the impact of the*

		transition to IPv6 on dynamic address assignment?
	Procedure:	Review the plan and look for a section dedicated to dynamic address assignment. At a minimum, it should indicate that there is no impact.
	Examples:	None.

G1591

Statement:	Prepare IPv6 Working Group products as part of the Internet Protocol Version 6 (IPv6) transition plan for a Node.
Rationale:	The Internet Protocol Version 6 (IPv6) Working Group has prescribed various products that can aid in the planning for the transition from Internet Protocol Version 4 (IPv4) to IPv6. The Node's Transition Plan should prepare these products to ensure that all the required activities are addressed.
Derived From	
Justifies	
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Are the Internet Protocol Version 6 (IPv6) Working Group products in the Node's Transition Plan?* **Procedure:** Look for the Working Group products in the Node's Transition Plan **Examples:** None.

G1592

Statement:	Include interoperability testing in the plan as part of the Internet Protocol Version 6 (IPv6) transition plan for a Node.
Rationale:	During the DoD transition period, a mixed IPv4/IPv6 environment will exist. Interoperability testing with both standards will ensure the Node can fully function during the transition period with all other

	Nodes.
Derived From	
Justifies	
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	
Evaluation Criteria:	**1. Test:** *Does the Node's IPv6 transition plan address interoperability testing in a mixed environment?* **Procedure:** Review the transition plan and verify that a test plan exists that specifically addresses interoperability testing in a mixed IP environment. **Examples:** None.

G1595

Statement:	Implement Domain Name System (DNS) to manage hostname/address resolution within the Node.
Rationale:	Domain Name System (DNS) servers should have replicated data from a DNS service that is outside the Node. The entries in the Server are fairly stable and updates can be sporadic. This should obviate any need for hard-coding Internet Protocol (IP) addresses within the Node.
Derived From	
Justifies	
Referenced By	Domain Name System (DNS)
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Is there a Domain Name System (DNS) server in the Node acquisition list?* **Procedure:** Look for a Domain Name System (DNS) server within the parts list for the Node.

		Examples:	None.
	2.	**Test:**	*Are there any hard coded Internet Protocol (IP) addresses within the source code or data files?*
		Procedure:	Look at the source code, properties files and descriptor files for the occurrence of Internet Protocol Version 4 (IPv4) or Internet Protocol Version 6 (IPv6) Internet Protocol (IP) addresses.
		Examples:	None.

G1596

Statement:	Use Domain Name System (DNS) Mail eXchange (MX) Record capabilities to configure electronic mail delivery to the Node.
Rationale:	Mail eXchange (MX) Record are defined to deliver mail to users within a domain. Every Node should provide its own Domain Name System (DNS) server. To support mail, it must have Mail eXchange (MX) Records defined in addition to the A or AAAA records. The MX record maps the domain name to a mail domain name. For example, email addresses or often defined like the following: **`joe@example.com`**. Alternatively, the email address could be defined as: **`joe@mail.example.com`**. The MX record enables this mapping of a domain name to a mail server name for a particular domain. The mail typically goes from an email client to an SMTP server. The SMTP server then looks for an MX record defined for the domain in the email address (i.e. **`example.com`**). If a domain name is defined in an MX record, the address associated with the domain name for a mail service is resolved and the mail is forwarded on to that address. See Oversimplified DNS for a more thorough explanation.
Derived From	
Justifies	
Referenced By	Domain Name System (DNS)
Acquisition Phase	Development, Oversight

Evaluation Criteria:	**1. Test:**	*Are there Mail eXchange (MX) Records defined within the Domain Name System (DNS)?*
	Procedure:	Look at the Domain Name System (DNS) records for Mail eXchange (MX) Records.
	Examples:	None.

G1598

Statement:	Allow dynamic Domain Name System (DNS) updates to the Node's internal DNS service by local Dynamic Host Configuration Protocol (DHCP) server(s).
Rationale:	There are two basic methods for assigning of Internet Protocol (IP) addresses within a network: static and dynamic. Static addresses are assigned to a particular system and never change. Dynamic Internet Protocol (IP) addresses are issued for a variable length of time: the "DCHP lease time." Dynamic Host Configuration Protocol (DHCP) is the principle mechanism used to assign and manage dynamic IP addresses. If the DHCP servers are allowed to update the Domain Name System (DNS), then the number of static addresses required by the system can be drastically reduced with preference being given to requesting services by domain name rather than IP address.
Derived From	
Justifies	
Referenced By	Domain Name System (DNS)
Acquisition Phase	Acquisition

Evaluation Criteria:	**1. Test:**	*Does the Domain Name System (DNS) server in the Node acquisition list support updates from Dynamic Host Configuration Protocol (DHCP) Servers?*
	Procedure:	Review the Domain Name System (DNS) server specification to confirm that it supports such operations.
	Examples:	None.

G1599

Statement:	Support both Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) simultaneously in the Node's Domain Name System (DNS) service.
Rationale:	During the transition period in the DoD community (FY06-FY15) networks, services and applications will be in a mixed environment. See Section 4.1, DoD Internet Protocol Version 6 (IPv6) Standard Profiles for IPv6 Capable Products. Internet Protocol Version 4 (IPv4). The Domain Name System (DNS) returns different address records depending on the Internet Protocol (IP) environment: A records for IPv4 or AAAA records for IPv6. A DNS must be able to support both.
Derived From	[G1590]
Justifies	
Referenced By	IPv4 to IPv6 Transition, Domain Name System (DNS)
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *Does the Domain Name System (DNS) server support both A Records and AAAA records?* **Procedure:** Review the Domain Name System (DNS)specification to confirm that it supports such both A and AAAA records. **Examples:** None.

G1600

Statement:	Obtain from DISA, in accordance with appropriate governing policy, any and all Internet Protocol Version 6 (IPv6) addresses used on DoD systems in the Node.
Rationale:	In order to maintain control and accountability on the network all the Internet Protocol (IP) addresses must be known. DISA is the clearing house for all addresses.
Derived From	[G1590]

Justifies	
Referenced By	IPv4 to IPv6 Transition, Domain Name System (DNS)
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *Is there a proper entry in the MILNIC for every IP address assigned to the system?* **Procedure:** Verify an adequate address allocation has been made in MILNIC for the system. **Examples:** None.

G1601

Statement:	Use configurable routers to provide dynamic Internet Protocol (IP) address management using Dynamic Host Configuration Protocol (DHCP).
Rationale:	There are two basic methods for assigning of Internet Protocol (IP) addresses within a network: static and dynamic. Static addresses are assigned to a particular system and never change. Dynamic IP addresses are issued for a variable length of time: the "DCHP lease time." Dynamic Host Configuration Protocol (DHCP) is the principle mechanism used to assign and manage dynamic IP addresses.
Derived From	
Justifies	
Referenced By	Routers, Multicast
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *Does the router in the Node acquisition list support Dynamic Host Configuration Protocol (DHCP)?* **Procedure:** Review the router specification to confirm that it supports such operations. **Examples:** None.

G1602

Statement:	Use configurable routers to provide static Internet Protocol (IP) addresses.
Rationale:	Some network Components such as the routers themselves and other security related services must reside on static Internet Protocol (IP) addresses. Serious comprises in the network can arise if these services are allowed to be dynamic.
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *Does the router in the Node acquisition list support static Internet Protocol (IP) addressing?* **Procedure:** Review the router specification to confirm that it supports such operations. **Examples:** None.

G1604

Statement:	Use configurable routers to provide time synchronization services using Network Time Protocol (NTP).
Rationale:	Over time, most computer clocks drift. Network Time Protocol (NTP) is one way to ensure that a computer clock stays accurate. Unfortunately, in order to stay synchronized, a network connection needs to be maintained. In environments that have limited bandwidth or poor quality of service (QoS) this can become a major issue.
Derived From	
Justifies	
Referenced By	Routers, Time Services
Acquisition Phase	Acquisition

Evaluation Criteria:	**1.**	**Test:**	*Does the router in the Node acquisition list support NTP Service?*
		Procedure:	Review the routers specification to confirm that it supports such operations.
		Examples:	None.

G1605

Statement:	Use configurable routers to provide multicast addressing.
Rationale:	Multicast addresses identify interfaces that allow a packet to be sent to all the addresses registered for the multicast service. This allows network to easily support applications such as collaboration, audio and video.
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Acquisition

Evaluation Criteria:	**1.**	**Test:**	*Does the router in the Node acquisition list support NTP Service?*
		Procedure:	Review the router specification to confirm that it supports such operations.
		Examples:	None.

G1606

Statement:	Manage routers remotely from within the Node.
Rationale:	Router manufactures routinely provide tools to enable remote configuration and management of the router. These tools are can speed and centralize the administration of the Nodes routers.
Derived From	
Justifies	

Referenced By	Routers
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *Does the router in the Node acquisition list support remote management?* **Procedure:** Review the router specification to confirm that it supports such operations. **Examples:** None.

G1607

Statement:	Configure routers according to National Security Agency (NSA) Router Configuration guidance.
Rationale:	The "Router Security Configuration Guide" provides technical guidance intended to help network administrators and security officers improve the security of their networks. It contains principles and guidance for secure configuration of Internet Protocol (IP) routers, with detailed instructions for Cisco System routers. The information presented can be used to control access, help resist attacks, shield other network Components, and help protect the integrity and confidentiality of network traffic.
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Is the Router Security Checklist complete and up to date?* **Procedure:** Check for the occurrence of the checklist and there should be a copy for every time the checklist has been completed. The checklist should indicate the date, time and results of the checklist with recommendation actions. **Examples:** Router Security Checklist

		This security checklist is designed to help review router security configuration and remind a user of any security areas that might be missed. ☐ Router security policy written, approved, distributed. ☐ Router IOS version checked and up to date. ☐ Router configuration kept off-line, backed up, access to it limited. ☐ Router configuration is well-documented, commented. ☐ Router users and passwords configured and maintained. ☐ Password encryption in use, enable secret in use. ☐ Enable secret difficult to guess, knowledge of it strictly limited. (if not, change the enable secret immediately) ☐ Access restrictions imposed on Console, Aux, VTYs. ☐ Unneeded network servers and facilities disabled. ☐ Necessary network services configured correctly (e.g. DNS) ☐ Unused interfaces and VTYs shut down or disabled. ☐ Risky interface services disabled. ☐ Port and protocol needs of the network identified and checked. ☐ Access lists limit traffic to identified ports and protocols. ☐ Access lists block reserved and inappropriate addresses. ☐ Static routes configured where necessary. ☐ Routing protocols configured to use integrity mechanisms. ☐ Logging enabled and log recipient hosts identified and configured. ☐ Router's time of day set accurately, maintained with NTP. ☐ Logging set to include consistent time information. ☐ Logs checked, reviewed, archived in accordance with local policy. ☐ SNMP disabled or enabled with good community strings and ACLs.

G1608

Statement:	Obtain the reference time for the Node time service from a globally synchronized time source.	
Rationale:	Currently Network Time Service is not a ubiquitous service across the Global Information Grid (GIG). Security directives prevent IP-based time synchronization across firewall boundaries (AFI 33-115, 16). An example of a precise globally synchronized time source is a Global Positioning System (GPS) system.	
Derived From		
Justifies		
Referenced By	Time Services	
Acquisition Phase	Acquisition	
Evaluation Criteria:	**1. Test:**	*Does the Node acquisition list include a precise globally synchronized time source such as Global Positioning System (GPS)*

		system?
	Procedure:	Review the acquisition list for a precise globally synchronized time source such as a Global Positioning System (GPS) system that can be used to accurately synchronize time.
	Examples:	None.

G1609

Statement:	Arrange for a backup time source for the Node time service.	
Rationale:	The most common type of backup time sources are crystal oscillators. The physical characteristics of the piezoelectric quartz crystal produce electrical oscillations at an extremely accurate frequency. This frequency can be used to mark time.	
Derived From		
Justifies		
Referenced By	Time Services	
Acquisition Phase	Acquisition	
Evaluation Criteria:	**1. Test:**	*Does the Node acquisition list include a backup time system?*
	Procedure:	Review the acquisition list for a backup time system that can be used to accurately synchronize time. For example: crystal oscillator, cesium or rubidium crystal oscillators. Crystal oscillator types and their abbreviations: MCXO microcomputer-compensated crystal oscillator OCVCXO oven-controlled voltage-controlled crystal oscillator OCXO oven-controlled crystal oscillator RbXO rubidium crystal oscillators (RbXO). TCVCXO temperature-compensated-voltage controlled crystal oscillator TCXO temperature-compensated crystal

	oscillator VCXO voltage-controlled crystal oscillator **Examples:** None.

G1610

Statement:	Configure the Dynamic Host Configuration Protocol (DHCP) services to assign multicast addresses.
Rationale:	When Dynamic Host Configuration Protocol (DHCP) services assign temporary Internet Protocol (IP) addresses to clients, the clients may wish to participate in a multicast service. Therefore, the DHCP service must support the assignment of multicast addresses as part of normal operations.
Derived From	
Justifies	
Referenced By	Multicast
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *Does the router in the Node acquisition list support the assignment of multicast Internet Protocol (IP) addresses as part of the normal Dynamic Host Configuration Protocol (DHCP) service?* **Procedure:** Review the router specification to confirm that it supports such operations. **Examples:** None.

G1611

Statement:	Implement IP gateways to interoperate with the Global Information Grid (GIG) until IP is supported natively for Components that are not Internet Protocol (IP) networked, such as aircraft data links (Link-16, SADL, etc.).
Rationale:	Component systems such as aircraft data links (Link-16, SADL, etc), should implement Transmission Control Protocol/Internet Protocol

	(TCP/IP) gateways to interoperate with the Global Information Grid (GIG) until TCP/IP is supported natively. This acts as an interim step that can be used to bridge the Internet Protocol (IP) divide.
Derived From	
Justifies	
Referenced By	Integration of Non- IP Transports
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Is there an Internet Protocol (IP) gateway in the system?* **Procedure:** Look at the code looking for Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP) or DDS code that will be front-ended by a gateway. **Examples:** None.

G1612

Statement:	Implement IP gateways as a service.
Rationale:	This does not mean that the service is a Web service or that it is limited to request/reply or other such usage patterns. In fact, for high-frequency data, such as track reporting, a function of the service could be to set up an out-of-band communication with a subscriber.
Derived From	
Justifies	
Referenced By	Integration of Non- IP Transports
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Is the gateway developed as a service that could be advertised in a registry?* **Procedure:** Examine the gateway and determine if it is a service.

	Examples: None.

G1613

Statement:	Prepare a Node to host new Component services developed by other Nodes or by the enterprise itself.
Rationale:	No matter how much space is available, there is always a need for more space. In the past, each system or application that was developed was often provided its own system resulting in an odd mix of monitors, racks and desktop machines tied together to accomplish a task. The result has been the push to more modular platform independent solutions that require standard frameworks that can support "pluggable" Components. If a solution anticipates that at some point in the future, it will need to either host an additional Component or become a Component in another Node. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Web Client Platform, Cross-Domain Interoperation
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Does the Node support the elements of a modern component based framework such as Java Platform, Enterprise Edition (Java EE), .NET or CORBA?* **Procedure:** Look for the existence of Java Platform, Enterprise Edition (Java EE), .NET or CORBA frameworks with in the Node's Component list or in its delivered software. **Examples:** None.

G1614

Statement:	Prepare a Node for the possibility of becoming a new Component

	service within another Node.
Rationale:	When a Node becomes a Component within another Node, there are many activities that become ancillary to original Node's mission. These activities need potentially need to be handled by the new hosting Node. This can be fairly painless if the original node implemented standard interfaces to the required activities. The node can than chose to provide proxies for these activities rather than the actual activity itself. These proxies are readily available for most standard interfaces. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Web Client Platform, Cross-Domain Interoperation
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Does the Node s use standardized interfaces to obtain the services of routine activities?* **Procedure:** Look for the existence of Java Platform, Enterprise Edition (Java EE), .NET or CORBA frameworks with in the Node's Component list or in its delivered software. **Examples:** None.

G1615

Statement:	Use Web browsers that support a wide breadth of browser technologies that can extend the browsers' functionality.
Rationale:	Web browsers are primarily designed to render HTML to the user. However, the limitations of static HTML were quickly realized and the functionality of the Web browsers were expanded to allow external extensions to the basic HTML processing. The first was the use of helper applications which eventually grew into the Common Client Interface (CCI). These did not prove to be powerful enough and three different methods were developed to extend the Web browser functionality: Web browser plug-ins, Web browser applications and

	scripting languages. Plug-ins' are a logical extension of the CCI approach. Web browser vendors provided APIs for application developers to use so their applications could be integrated into the Browser. This approach though somewhat successful was plagued by the incompatibilities between the Web browser vendor's APIs. This required a phenomenal amount of work to be compliant with the various vendors and the different vendor releases. The second approach allowed developers to actually embed the extension software directly into their web pages. This is subject to vendor's client security philosophy. For example, Microsoft's ActiveX objects, run natively within Microsoft Internet Explorer, are executed in a very unrestricted virtual machine environment. Java Applet virtual machines are more restrictive in nature and do not allow access to the client disk drive, allow unrestricted network call backs. The last method of extending the browser functionality is through the use of lightweight scripting languages such as JavaScript, JScript and VBScript. This approach seems to be the one that recently has received the most support. JavaScript is non-vendor specific while JScript and VBScript are specific to Microsoft. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Browser
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Web browser support plug-ins, APIs and scripting languages?* **Procedure:** Review the list of tested Web browsers and make sure they support plug-ins, APIs and scripting languages. **Examples:** None.

G1618

Statement:	Configure servers with a Common Access Card (CAC) reader.
Rationale:	The DoD Instruction 8520.2 on Public Key Infrastructure (PKI) and Public Key (PK) Enabling defines CAC applicability and scope: *This Instruction applies to:* *2.4. All DoD unclassified and classified information systems including networks (e.g., Non-secure Internet Protocol (IP) Router Network , Secret Internet Protocol Router Network, Web servers, and e-mail systems. Excluded are Sensitive Compartmented Information, and information systems operated within the Department of Defense that fall under the authority of the Director of Central Intelligence Directive (DCID) 6/3 (reference (h)).* ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Common Access Card (CAC) Reader
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do all the client and server hardware come equipped with Common Access Card (CAC) Readers?* **Procedure:** Review the hardware list and verify that all hardware comes with or has external CAC readers. **Examples:** None. **2. Test:** *Does the server pass the security scans?* **Procedure:** Apply a D0D-approved security scan to the server and check the results to see that the server passes the scan.

	Examples: None.

G1619

Statement:	Configure clients with a Common Access Card (CAC) reader.
Rationale:	The DoD Instruction 8520.2 on Public Key Infrastructure (PKI) and Public Key (PK) Enabling defines Common Access Card (CAC) applicability and scope: *This Instruction applies to:* *2.4. All DoD unclassified and classified information systems including networks (e.g., Non-secure Internet Protocol (IP) Router Network , Secret Internet Protocol Router Network, Web servers, and e-mail systems. Excluded are Sensitive Compartmented Information, and information systems operated within the Department of Defense that fall under the authority of the Director of Central Intelligence Directive (DCID) 6/3 (reference (h)).* ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Common Access Card (CAC) Reader
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do all the client and server hardware come equipped with Common Access Card (CAC) Readers?* **Procedure:** Review the hardware list and verify that all hardware comes with or has external CAC readers. **Examples:** None. **2. Test:** *Does the server pass the security scans?*

	Procedure: Apply a D0D-approved security scan to the server and check the results to see that the server passes the scan. **Examples:** None.

G1621

Statement:	Allow all Components that are hosted at a Node to access and use the Node's Web infrastructure.
Rationale:	A Web application infrastructure includes those elements which allow an application developer to deploy their application at a Node without regard to how the application will display results to an end user, execute or be deployed. There are many choices available to a application and not providing a common Web application infrastructure will result in wasteful, duplicate and often conflicting capabilities at each Node. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Web Infrastructure
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does Node acquisition list include duplicate Web application infrastructure elements?* **Procedure:** Review the acquisition list for web application infrastructure elements (Web Portal, Web Server and Web Application Containers). **Examples:** None.

G1622

Statement:	Implement commercial off-the-shelf (COTS) virus scanning and worm detection software, along with accompanying capabilities for update of software and virus definitions, on each client or server

	hardware in the Node in accordance with the Desktop Applications STIG.
Rationale:	The viral and worm assault on computing resources is major concern but is not strictly limited to DoD hardware and operating systems. It has become a ubiquitous, wide spread problem that spreads destruction indiscriminately. Since the problem is not strictly a DoD problem, commercial off-the-shelf (COTS) solutions are always being updated to meet the current threats and are essential in protecting the assets. All hardware platforms should employ virus and worm detection and removal software that is routinely run (especially on hardware the runs Microsoft products). ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Host Information Assurance
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do all hardware devices listed in the Node acquisition list have COTS licensed virus and worm detection software?* **Procedure:** Review the Node acquisition list and make sure there is one license for each piece of computer hardware. **Examples:** None. **2. Test:** *Do all hardware devices listed in the Node acquisition list have COTS virus and worm detection software installed?* **Procedure:** Review the prerequisites in the installation manual for virus and worm software. **Examples:** None.

G1623

Statement:	Implement personal firewall software on client or server hardware used for remote connectivity in accordance with the Desktop Applications STIG, Network STIG, and Enclave STIG.
Rationale:	All hardware that is plugged into a network is subject to attack by hackers. In addition to hardware firewalls, every piece of hardware should be protected by a software firewall. These firewalls continuously monitor the activity on the network port and detect possible hostile attacks. Hostile attacks can be permanently blocked or blocked for a particular occasion at the discretion of the user. Since this problem is not restricted to DoD assets, Commercial off-the-shelf (COTS) products are continuously being updated to meet the latest threats and are essential in meeting these threats. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Host Information Assurance
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do all the hardware devices listed in the Node acquisition list have COTS software firewall licensed software?* **Procedure:** Review the Node acquisition list and make sure there is one license for each piece of computer hardware. **Examples:** None. **2. Test:** *Do all hardware devises listed in the Node acquisition list have COTS firewall software installed and is it enabled?* **Procedure:** Review the prerequisites in the installation manual for firewall software. **Examples:** None.

G1624

Statement:	Install anti-spyware on all client and server hardware.
Rationale:	The following discussion of spyware is from Wikipedia on 3 April 2006. *In the field of computing, the term spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. While the term taken literally suggests software that surreptitiously monitors the user, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party.* *Spyware differs from viruses and worms in that it does not usually self-replicate. Like many recent viruses, however, spyware – by design – exploits infected computers for commercial gain. Typical tactics furthering this goal include delivery of unsolicited pop-up advertisements; theft of personal information (including financial information such as credit card numbers); monitoring of Web-browsing activity for marketing purposes; or routing of HTTP requests to advertising sites.* *As of 2005,* ***spyware has become one of the pre-eminent security threats to computer-systems running Microsoft Windows operating-systems (and especially to users of Internet Explorer because of that browser's dependence on the Windows operating system).*** *Some malware on the Linux and Mac OS X platforms has behavior similar to Windows spyware, but to date has not become anywhere near as widespread.* **Note***:* This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Host Information Assurance

Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do all the hardware devises listed in the Node acquisition list have COTS software anti-spyware licensed software?* **Procedure:** Review the Node acquisition list and make sure there is one license for each piece of computer hardware.. **Examples:** None. **2. Test:** *Do all hardware devises listed in the Node acquisition list have COTS anti-spyware software installed and is it enabled?* **Procedure:** Review the prerequisites in the installation manual for firewall software. **Examples:** None.

G1625

Statement:	Provide a commercial off-the-shelf Directory Service that all of the Components of a Node can use.
Rationale:	A Directory Service is a service that stores information about a computer network. It stores information about the network users as well as information about locations on a computer network also called network shares. ***Note***: This guidance is provisional pending completion of detailed review. The following is a list of possible Directory Service vendors provided by Wikipedia. The following is a partial list of Directory vendors that was taken from Wikipedia. **NIS** The Network Information Service (NIS) protocol, originally named Yellow Pages (YP) was Sun Microsystem's implementation of a directory service for Unix network environments. (Sun has, in the early 2000s, merged its iPlanet alliance Netscape and developed its Lightweight Directory Access Protocol

		(LDAP)-based directory service to become part of Sun ONE, now called Sun Java Enterprise.)
	eDirectory	This is Novell's implementation of directory services. It supports multiple architectures including Windows, Netware, Linux and several flavors of Unix and has long been used for user administration, configuration management, and software management. eDirectory has evolved into a central component in a broader range of Identity Management products. It was previously known as Novell Directory Services.
	Red Hat Directory Server	Red Hat released the directory service that it acquired from Netscape Security Solutions as a commercial product running on top of Red Hat Enterprise Linux called Red Hat Directory Server and as part of Fedora Core called Fedora Directory Server.
	Active Directory	Microsoft's directory service is the Active Directory which is included in the Windows 2000 and Windows Server 2003 operating system versions.
	Open Directory	Apple's Mac OS X Server offers a directory service called Open Directory which integrates with many open standard protocols such as Lightweight Directory Access Protocol (LDAP) and Kerberos as well as proprietary directory solutions like Active Directory and eDirectory.
	open-source tools	OpenLDAP and the Kerberos (protocol), and Samba software which can act as a Domain Controller with Kerberos and Lightweight Directory Access Protocol (LDAP) backends.
Derived From		
Justifies		
Referenced By	Directory Services	
Acquisition Phase	Acquisition, Development, Oversight	
Evaluation Criteria:	**1. Test:**	*Is there a COTS directory service listed in the Node acquisition list?*
	Procedure:	Review the Node acquisition list and make sure there is one license for a directory service.
	Examples:	None.

	2. Test:	*Is an Open Source directory service going to be used?*
	Procedure:	Review the prerequisites in the installation manual for open source directory service software.
	Examples:	None.

G1626

Statement:	Identify which Core Enterprise Services (CES) capabilities the Node Components require.
Rationale:	In an ideal world, all the Core Enterprise Service (CES) capabilities would be available at all the Nodes immediately. This would allow all Components to be deployed at any Node. The reality is that this is too costly and wasteful of the limited resources (human and non-human) available to each Node. Identifying which CES capabilities are essential in supporting the COI driven Components is a requisite for success. ***Note*:** The guidance calls out for the capabilities, not just the CES. Each individual CES is extremely complex unto itself and understanding which subset of capabilities is important in supporting the Component. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	CES Definitions and Status
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the list of Components that comprise the Node indicate which CES capabilities are required to deploy each Component?* **Procedure:** Review the list of Components and verify that they have indicated which CES capabilities are required to support the Component.

	Examples: None.

G1627

Statement:	Identify the priority of each Core Enterprise Services (CES) capability the Node Components require.
Rationale:	In balancing the needs of the Node's Components, it is important to know what the priority is of getting a CES available on the Node. Some capabilities are "essential" at getting a Component Deployed at a Node. Some are essential for a particular Component increment. This helps the Node have a schedule that can support the transition or evolution of the current federation of systems to the Global Information Grid (GIG) vision. It minimizes the risk to the individual Component and the Node as a whole. ***Note*:** The guidance calls out for the capabilities, not just the CES. Each individual CES is extremely complex unto itself and understanding which subset of capabilities is important in supporting the Component. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	CES Definitions and Status, CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the list of Components that comprise the Node indicate the priority of the CES capabilities either relative to each other or as of a date?* **Procedure:** Review the list of Components and verify that they have indicated what the priority of the CES capabilities either relative to each other or as of a date. **Examples:** None.

G1628

Statement:	Identify which Net-Centric Enterprise Services (NCES) capabilities the Node requires.
Rationale:	The Net-Centric Enterprise Services (NCES), when it is complete, will offer a complete tableau of capabilities and services that a Node can use depending on the suitability of the services to the Node's environment. For example, when the Node is not deployed, it may rely on proxies to the NCES services. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	CES Definitions and Status
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node have a list of Net-Centric Enterprise Services (NCES) capabilities that it depends on when not deployed?* **Procedure:** Review the Node's documents for a list of Net-Centric Enterprise Services (NCES) capabilities required by the Node when not deployed. **Examples:** None.

G1629

Statement:	Identify which Net-Centric Enterprise Services (NCES) capabilities the Node requires during deployment.
Rationale:	Relying on a high-bandwidth Transmission Control Protocol/Internet Protocol (TCP/IP) network connection is not a reality for many deployed Nodes. These Nodes will have to develop many of their own CES capabilities for use by their member Components while deployed. When the Node is not deployed, it may rely on proxies to the Net-Centric Enterprise Services (NCES) services.

	Note: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	CES Definitions and Status
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node have a list of Net-Centric Enterprise Services (NCES) capabilities that it depends on while deployed?* **Procedure:** Review the Node's documents for a list of Net-Centric Enterprise Services (NCES)capabilities required by the Node while deployed. **Examples:** None.

G1630

Statement:	Comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) for implemented Core Enterprise Services (CES) in the Node.
Rationale:	When a CES is implemented locally, the Global Information Grid (GIG) Key Interface Profiles (KIPs) developed by DISA should be used as the authoritative definition of the interfaces. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	[G1637], [G1641], [G1643], [G1644]
Referenced By	CES and Intermittent Accessibility, Key Interface Profile (KIP)
Acquisition Phase	Development, Oversight

Evaluation Criteria:	**1.**	**Test:**	*Do all CES used locally within the Node implement the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?*
		Procedure:	Verify that the interfaces for Core Enterprise Services (CES) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that CES.
		Examples:	None.

G1631

Statement:	Expose Core Enterprise Services (CES) that comply with the applicable Global Information Grid (GIG) Key Interface Profiles (KIPs) in all Node services proxies.
Rationale:	A Node may expose or control access to Global Information Grid (GIG) CES by using proxies. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	[G1638], [G1642], [G1646]
Referenced By	CES and Intermittent Accessibility, Key Interface Profile (KIP)
Acquisition Phase	Development, Oversight

Evaluation Criteria:	**1.**	**Test:**	*Do all CES proxies locally defined within the Node expose CES using the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?*
		Procedure:	Verify that the interfaces for CES proxies follow Key Interface Profiles (KIPs) for that Global Information Grid (GIG) KIP.
		Examples:	None.

G1632

Statement:	Certify and accredit Nodes with all applicable DoD Information Assurance (IA) processes.
Rationale:	Nodes are part of the DoD Global Information Grid (GIG) and are consequently required to have DoD Information Assurance (IA) certification and accreditation. Details for certification and accreditation are specified in DoD Directive 8500.1, DoD Instruction 8500.2, DoD Directive 8580.1, and DoD Instruction 5200.40. Satisfaction of these requirements results in IA compliance verification of the Node. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Information Assurance (IA)
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node have IA certification and accreditation?* **Procedure:** Ask to examine the certification and accreditation reports. **Examples:** None.

G1633

Statement:	Host only DoD Information Assurance (IA) certified and accredited Components.
Rationale:	Nodes that expose the external Node users to non-certified or non-accredited Components are very risky to the stability of the entire Node network. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	

Justifies	
Referenced By	Information Assurance (IA)
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node have a plan to scan all Components on a routine basis?* **Procedure:** Look for a plan and examine the results of the scan. **Examples:** None.

G1634

Statement:	Certify and accredit Components with all applicable DoD Information Assurance (IA) processes.
Rationale:	Each Component could theoretically be deployed on any Node. Therefore, it is the responsibility of the Component to be DoD Information Assurance (IA) certified and accredited. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Information Assurance (IA)
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Are all the Components DoD Information Assurance (IA) certified and accredited?* **Procedure:** Examine the certification and accreditation reports. **Examples:** None.

G1635

Statement:	Make Nodes that will be part of the Global Information Grid (GIG) consistent with the GIG Integrated Architecture.
Rationale:	The Global Information Grid (GIG) architecture describes the basic, high level architecture in which Nodes reside. It is an integrated architecture consisting of the various DoDAF views. It provides a common lexicon and defines a basic infrastructure for the performance of information exchanges with other GIG Nodes using the GIG Enterprise Services (GES) and the Net-Centric Enterprise Services (NCES). The GIG Architecture can be viewed at https://disain.disa.mil/ncow/gigv2/index.htm. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Integrated Architectures
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Are there DoDAF integrated architecture products defined for the Node?* **Procedure:** Look for the occurrence of Operational View (OV), Systems View (SV), Technical Standards View (TV) and All Views (AV). **Examples:** None.

G1636

Statement:	Comply with the Net-Centric Operations and Warfare Reference Model (NCOW RM).
Rationale:	The Net-Centric Operations and Warfare Reference Model (NCOW RM) is focused on achieving net-centricity. Compliance with the NCOW RM translates to articulating how each Node approaches and implements net-centric features. Compliance does not require separate documentation; rather, it requires that a Node address, within existing architecture, analysis, and program architecture documentation, the

	issues identified by using the model, and further, that they make explicit the path to net-centricity the program is taking. Node compliance with the NCOW RM is demonstrated through inspection and analysis. • Use of NCOW RM definitions and vocabulary; • Incorporation of NCOW RM Operational View (OV) capabilities and services in the materiel solution; • Incorporation of NCOW RM Technical View Information Technology (IT) and National Security Systems (NSS) standards in the Technical View products developed for the materiel solution. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Net-Centric Operations and Warfare Reference Model (NCOW RM)
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	**1. Test:** *Have the instructions in the Defense Acquisition University (DAU) Guidebook section 7.2.6 been used to check the Node for NCOW RM compliance?* **Procedure:** Check Node documentation. **Examples:** **2. Test:** *Have the instructions in Chairman of the Joint Chiefs of Staff Instruction (CJCS) Instruction 3170.01been used to check the Node for Net-Centric Operations and Warfare Reference Model (NCOW RM) compliance?* **Procedure:** Check Node documentation. **Examples:** **3. Test:** *Have the instructions in Chairman of the Joint Chiefs of Staff Instruction (CJCS) Instruction 6212.01 been used to check the Node for Net-Centric Operations and Warfare Reference*

	Model (NCOW RM) compliance? **Procedure:** Check Node documentation. **Examples:**

G1637

Statement:	Make Node-implemented directory services comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs).
Rationale:	When directory services are implemented locally, the Global Information Grid (GIG) Kips developed by DISA should be used as the authoritative definition of the interfaces. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	[BP1630]
Justifies	
Referenced By	Directory Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Do all directory services used locally within the Node implement the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?* **Procedure:** Verify that the interfaces for directory services implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that directory services. **Examples:** None.

G1638

Statement:	Comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node directory services proxies.

Rationale:	A Node may expose or control access to Global Information Grid (GIG) directory services by using proxies. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	[BP1631]
Justifies	
Referenced By	Directory Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Do all directory services proxies locally defined within the Node expose directory services using the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?* **Procedure:** Verify that the interfaces for directory services proxies follow Key Interface Profiles (KIPs) for that Global Information Grid (GIG) KIPs. **Examples:** None.

G1639

Statement:	Describe Components exposed by the Node as specified by the Service Definition Framework (SDF).
Rationale:	The construction of registry entries is specified by the Service Definition Framework (SDF) documented in Net-Centric Implementation Directives (NCIDs) S300. The common Service Definition Framework that serves as the basis for adequately describing the offered Component service from both a provider's and consumer's perspective. It describes the contract between the Component service provider and the Component service consumer, and serves as the basis for a Service Level Agreements (SLA). The common service definition framework consists of elements that include interface, service level, security and implementation information.

	Note: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Service Discovery
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Is there a Service Definition Framework (SDF) available for each of the Components' Services exposed through the Node?* **Procedure:** Look for a Service Definition Framework (SDF) for each Component service exposed through the Node. **Examples:** None.

G1640

Statement:	Register Components exposed by the Node with the DISA-hosted registries.
Rationale:	The best way to for an exposed Node's Component service to be discovered is by being registered in the DISA registry. The DISA registry implementation uses Universal Description, Discovery, Integration (UDDI). ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Service Discovery
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Is the exposed Node's Component's service registered in the DISA Universal Description,*

	Discovery, Integration (UDDI) Registry? **Procedure:** Examine the DISA Universal Description, Discovery, Integration (UDDI) Registry and look for the exposed Node's Component's service. **Examples:** None.

G1641

Statement:	Comply with the Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node-implemented Service Discovery (SD).
Rationale:	When a Service Discovery (SD) is implemented locally, the Global Information Grid (GIG) Kips developed by DISA should be used as the authoritative definition of the interfaces. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	[BP1630]
Justifies	
Referenced By	Service Discovery
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Service Discovery (SD) used locally within the Node implement the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?* **Procedure:** Verify that the interfaces for Service Discovery (SD) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that Service Discovery. **Examples:** None.

G1642

Statement:	Comply with the Service Discovery Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node Service Discovery (SD) proxies.
Rationale:	A Node may expose or control access to Global Information Grid (GIG) Service Discovery (SD) by using proxies. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	[BP1631]
Justifies	
Referenced By	Service Discovery
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Do the Service Discovery (SD) proxies locally defined within the Node expose Service Discovery using the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?* **Procedure:** Verify that the interfaces for Service Discovery (SD) proxies follow KIPs for that Global Information Grid (GIG) Key Interface Profiles (KIPs). **Examples:** None.

G1643

Statement:	Comply with the Federated Search – Registration Web Service (RWS) Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node implemented Federated Search – Registration Web Service (RWS).
Rationale:	When a Federated Search – Registration Web Service (RWS) is implemented locally, the Global Information Grid (GIG) KIPs developed by DISA should be used as the authoritative definition of the interfaces. This allows a Component that is hosted by one Node to

	be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	[BP1630]
Justifies	
Referenced By	Content Discovery Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does a Federated Search – Registration Web Service (RWS) used locally within the Node implement the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?* **Procedure:** Verify that the interfaces for Federated Search – Registration Web Service (RWS) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that Federated Search – Registration Web Service (RWS). **Examples:** None.

G1644

Statement:	Comply with the Federated Search – Search Web Service (SWS) Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node implemented Federated Search – Search Web Service (SWS).
Rationale:	When a Federated Search – Search Web Service (SWS) is implemented locally, the Global Information Grid (GIG) Key Interface Profiles (KIPs) developed by DISA should be used as the authoritative definition of the interfaces. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	[BP1630]
Justifies	

Referenced By	Content Discovery Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does Federated Search – Search Web Service (SWS) used locally within the Node implement the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?* **Procedure:** Verify that the interfaces for Federated Search – Search Web Service (SWS) implement Global Information Grid (GIG) Key Interface Profiles (KIPs) for that Federated Search – Search Web Service (SWS). **Examples:** None.

G1645

Statement:	Implement a local Content Discovery Service (CDS).
Rationale:	The node should implement the Content Discovery Service (CDS) as part of the node infrastructure to be shared among the Components hosted at the Node. The content is normally provided by the systems within the Node. However, if a Node is frequently disconnected, has intermittent connectivity, or is otherwise isolated, it seems improbable that there would be any significant value in hosting a local implementation of this capability. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Content Discovery Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node implement the Content Discovery Service (CDS) Global Information Grid (GIG) Key Interface Profile (KIP)?*

	Procedure:	Look for an implementation at the Node of the Content Discovery Service (CDS) Global Information Grid (GIG) Key Interface Profiles (KIPs).
	Examples:	None.

G1646

Statement:	Comply with the directory services Global Information Grid (GIG) Key Interface Profiles (KIPs) in Node Federated Search Services proxies.	
Rationale:	A Node may expose or control access to Global Information Grid (GIG) Federated Search Services by using proxies. This allows a Component that is hosted by one Node to be hosted on another node with a minimal impact. ***Note***: This guidance is provisional pending completion of detailed review.	
Derived From	[BP1631]	
Justifies		
Referenced By	Content Discovery Services	
Acquisition Phase	Development, Oversight	
Evaluation Criteria:	**1. Test:**	*Do all Federated Search Services proxies locally defined within the Node expose Federated Search Services using the applicable Global Information Grid (GIG) Key Interface Profile (KIP)?*
	Procedure:	Verify that the interfaces for Federated Search Services proxies follow KIPs for that Global Information Grid (GIG) Key Interface Profiles (KIPs).
	Examples:	None.

G1647

Statement:	Provide access to the Federated Search Services.

Rationale:	Content Discovery Service can search across a set of Content Discovery Services and yield an integrated result. The current approach to providing this service is to harness an existing capability termed "Federated Search" developed under the Horizontal Fusion (HF) program. The capability utilizes the DoD Discovery Metadata Specification (DDMS). ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Content Discovery Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Does the Node provide access to the Federated Search Service Global Information Grid (GIG) Key Interface Profile (KIP)?* **Procedure:** Look for a proxy or an implementation that provides access to the "Federated Search" capabilities. **Examples:** None.

G1648

Statement:	Host the Registration Web Service (RWS) registration portlet in the Node.
Rationale:	The process of registering a Node's Component service with the Registration Web Service (RWS) can be quite complicated. By providing access to the registration portlet the chances of obtaining a registration and of having valid data in the registration are greatly increased. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	

Referenced By	Content Discovery Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Is the Registration Web Service (RWS) registration portlet hosted on the local Node?* **Procedure:** Look for the Registration Web Service (RWS) registration portlet implementation. **Examples:** None.

G1649

Statement:	Specifically include provisions for incremental implementation of the CES services.
Rationale:	The states of the individual services that comprise the CES are at different level of maturity. Consequently, an incremental approach allows Node development to continue in parallel with the CES functionality. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Is there an incremental development approach?* **Procedure:** Review the Node's schedule for incremental development. **Examples:** None.

G1650

Statement:	Specifically include provisions for incremental implementation of the hosting Node's CES services for Node Components.
Rationale:	The states of the individual services that comprise the CES are at different level of maturity. Consequently, an incremental approach allows Component development to continue in parallel with the Node and CES functionality. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Is there an incremental development approach?* **Procedure:** Review the schedule for Components for incremental development. **Examples:** None.

G1651

Statement:	Do not implement server side CES functionality for Components.
Rationale:	The burden of aligning to standard CES functionality and providing the functionality uniformly rests on the Node infrastructure, rather than the Components within the Node. This isolates the Components from the CES complexity and enhancing portability and interoperability of the Components. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	

Referenced By	CES and Intermittent Accessibility
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Do any Component systems, applications or services implement and of the server side CES Global Information Grid (GIG) Key Interface Profiles (KIPs)?* **Procedure:** Review the Component systems, applications or services code for implementations of the server side CES Global Information Grid (GIG) Key Interface Profiles (KIPs). **Examples:** None.

G1652

Statement:	Use DoD PKI X.509 certificates for servers.
Rationale:	Using a DoD PKI X.509 server certificate identifies the server as being trusted by the DoD and guarantees that the server's identity is legitimate. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Identity Management
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** *Is the server certificate a valid DoD PKI X.509 certificate that is non-expired?* **Procedure:** Open the server certificate and check that it is trusted by a trusted DoD root certificate. **Examples:**

Best Practice Details

BP1594

Statement:	Implement IETF RFC 1323 for high bandwidth, high latency satellite communications.
Rationale:	If high bandwidth, high latency satellite communications are employed, the Node should implement IETF RFC 1323, which addresses describes adjustment of the Transmission Control Protocol/Internet Protocol (TCP/IP) sliding window buffer to accommodate large amounts of transmitted data that may be in the pipe and not yet unacknowledged due to the long round-trip times of such links. ***Note***: This guidance is provisional pending completion of detailed review.
Derived From	
Justifies	
Referenced By	Mobile Nodes
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *If the system is involved in high bandwidth, high latency satellite communications, does the Node design specify implementation and adherence to explicitly IETF RFC 1323?* **Procedure:** Determine if parts of the system involve high bandwidth, high latency satellite communications and if so, look for IETF RFC 1323 references in the Node's design. **Examples:** None.

BP1597

Statement:	Consider operational performance constraints in the design of the Node's Domain Name System (DNS).

Rationale:	Operational performance constraints such as narrow band width or intermittent service can have a large impact in how the Domain Name System (DNS) server is configured and consequently on the DNS chosen to support the Node.
Derived From	
Justifies	
Referenced By	Domain Name System (DNS)
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** *Have the operational performance constraints been delineated and used to justify the Domain Name System (DNS) used by the Node?* **Procedure:** Review the acquisition documents looking for justifications for the selection of the Domain Name System (DNS). **Examples:** None.

BP1603

Statement:	Configure routers to provide static addresses as defined by the Network Security Technical Implementation Guide (STIG).
Rationale:	
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1653

Statement:	Do not build dedicated Node guard products.
Rationale:	
Derived From	
Justifies	
Referenced By	Trusted Guards
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1654

Statement:	Do not build dedicated Component guard products.
Rationale:	
Derived From	
Justifies	
Referenced By	Trusted Guards
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1660

Statement:	Describe the potential impacts in the Service Registry for services developed to utilize Internet Protocol Version 6 (IPv6) features which

	may perform differently if accessed via an Internet Protocol Version 4 (IPv4) infrastructure.
Rationale:	
Derived From	
Justifies	
Referenced By	IPv4 to IPv6 Transition
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1661

Statement:	Engage with the Net-Centric Enterprise Services (NCES) program office to explore approaches for mobile use of the Core Enterprise Services (CES) services in mobile Nodes that rely on Transmission Control Protocol/Internet Protocol (TCP/IP) for inter-node communication.
Rationale:	
Derived From	
Justifies	
Referenced By	CES Definitions and Status
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1662

Statement:	Follow the guidance provided in the Security Technical Implementation Guide (STIG) for Domain Name System (DNS) implementations.
Rationale:	The STIG addresses implementation options such as the choice of basic DNS server types (primary, secondary, caching-only), use of a split-DNS design, location of servers in the network and relationship to other network components, secure administration, security of zone transfers, and initial configuration.
Derived From	
Justifies	
Referenced By	Domain Name System (DNS)
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1663

Statement:	Design a Domain Name System (DNS) in coordination with the appropriate governing Internet Protocol Version 6 (IPv6) Transformation Office.
Rationale:	
Derived From	
Justifies	
Referenced By	Domain Name System (DNS)
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:**

	Procedure: **Examples:**

BP1664

Statement:	Configure routers in accordance with the National Security Agency (NSA) Router Security Configuration Guide.
Rationale:	The National Security Agency (NSA) Router Security Configuration Guide is based on the best practices from major WAN device suppliers (i.e., Cisco and Juniper).
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1665

Statement:	Configure routers to update the Node's internal DNS service in accordance with the Network Security Technical Implementation Guide (STIG).
Rationale:	
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Development, Oversight

Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1667

Statement:	Implement a Virtual Private Network (VPN) in accordance with the guidance provided in the Network STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Virtual Private Networks (VPN)
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1668

Statement:	Acquire and configure guard products with the help of the Government program offices that acquire such guards.
Rationale:	
Derived From	
Justifies	
Referenced By	Trusted Guards
Acquisition Phase	
Evaluation Criteria:	**1. Test:**

	Procedure: **Examples:**

BP1669

Statement:	Use XML-capable guards in anticipation that net-centric solutions through guards will rely heavily on the passing of XML messages.
Rationale:	
Derived From	
Justifies	
Referenced By	Trusted Guards
Acquisition Phase	
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1670

Statement:	Monitor Black Core implementation issues and prepare a plan for local implementation in coordination with system programs fielded within the Node.
Rationale:	
Derived From	
Justifies	
Referenced By	Black Core
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:**

	Procedure: **Examples:**

BP1671

Statement:	Consider Black Core transition whenever there is a significant Node network design or configuration decision to make in an effort to avoid costly downstream changes caused by Black Core transition.
Rationale:	
Derived From	
Justifies	
Referenced By	Black Core
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1672

Statement:	Be prepared to integrate fully with the Information Assurance (IA) infrastructure.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Client Platform
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:**

	Procedure: **Examples:**

BP1673

Statement:	Be prepared to integrate fully with the Enterprise Management Services (EMS) infrastructure.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Client Platform
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1674

Statement:	Configure the browser in accordance with the Web Server Security Technical Implementation Guide (STIG), Desktop Applications STIG, and Windows 2003/XP/2000 Addendum STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Browser
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:**

	Procedure: **Examples:**

BP1675

Statement:	In the Node's Web infrastructure, support the technologies and standards used by the CES services under development as well as any technologies and standards used for Community of Interest (COI) services.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Infrastructure, CES Definitions and Status
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1677

Statement:	Consider using Web proxy servers and load balancers.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Infrastructure
Acquisition Phase	Acquisition, Development
Evaluation Criteria:	1. **Test:**

	Procedure: **Examples:**

BP1679

Statement:	Implement a Node that uses Active Directory (AD) in accordance with the recommendations of the DoD Active Directory Interoperability Working Group (DADIWG).
Rationale:	The purpose of DoD Active Directory Interoperability Working Group (DADIWG) specification is to define a DoD naming convention for users with the objective of promoting more efficient data synchronization to support email communications for the Joint environment and to prepare Active Directory to support more sophisticated DoD-wide directory and discovery services. This specification develops consistent naming conventions – naming formats, content, and supporting data values, for a baseline set of attributes for Active Directory User Objects.
Derived From	
Justifies	
Referenced By	Domain Directories
Acquisition Phase	Development, Oversight
Evaluation Criteria:	1. **Test:** **Procedure:** **Examples:**

BP1680

Statement:	Instrument Component services that a Node exposes to the Global Information Grid (GIG) to collect performance metrics.
Rationale:	In a dynamic environment, where services and information exchange partners may be dynamic, metrics can be a key factor in the selection of services. Performance metrics that are advertised externally and frequently updated allow potential service users the ability to select an implementation that meets their performance requirements, such as a

	measurement of reliability. Standards for metrics are expected to be defined in the Net-Centric Implementation Directives (NCID) S500 document that is not yet available. Some draft metrics that may be appropriate for web services are given in the following table: **SLA Metric** / **Metric Description** **Availability** — How often is the service available for consumption? **Accessibility** — How capable is the service of serving a client request now? **Performance** — How long does it take for the service to respond? **Compliance** — How fully does the service comply with stated standards? **Security** — How safe and secure is it to interact with this service? **Energy Efficiency** — How energy-efficient is this service for mobile applications? **Reliability** — How often does the service fail to maintain its overall service quality?
Derived From	
Justifies	
Referenced By	Instrumentation for Metrics
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1681

Statement:	Make Component services metrics visible and accessible as part of the service registration and updated periodically.
Rationale:	Metrics are normally also needed to ensure performance is provided according to more traditional Service Level Agreements (SLAs), and for operations management.

Derived From	
Justifies	
Referenced By	Instrumentation for Metrics
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1683

Statement:	Coordinate the Node schedule with the Net-Centric Enterprise Services (NCES) schedule.
Rationale:	An unavoidable consequence of the Node architecture, is that the CES being developed by Net-Centric Enterprise Services (NCES) is occurring in parallel with the development of the Nodes themselves. If the Node's schedule is not coordinated with NCES, Node capabilities will be developed that can not be supported within the NCES infrastructure.
Derived From	
Justifies	
Referenced By	CES Definitions and Status, CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** *Is there a Node roadmap that maps to the Net-Centric Enterprise Services (NCES) schedule?* **Procedure:** Look for a document that cross-references the Net-Centric Enterprise Services (NCES) schedule of capabilities to the Node's schedule. **Examples:** None

BP1684

Statement:	Coordinate the Node schedule with the Component schedules.
Rationale:	All schedules are subject to slippage or modifications due to changing priorities. If the Net-Centric Enterprise Services (NCES) schedule changes or the development of certain Node capabilities is changed, there can be an impact to a Node's Component's schedules.
Derived From	
Justifies	
Referenced By	CES Definitions and Status, CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1685

Statement:	For Key Interface Profile (KIP) specifications that are not available or insufficiently mature, implement a "best effort" by following the published intent of functionality and monitor or participate in the relevant specification development body.
Rationale:	
Derived From	
Justifies	
Referenced By	Key Interface Profile (KIP)
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** **Procedure:**

	Examples:

BP1686

Statement:	Align Node interfaces to Components for directory services with the guidance being provided by the JEDIWG and sub-working groups, including such guidance as naming conventions, federation, and synchronization.
Rationale:	
Derived From	
Justifies	
Referenced By	Directory Services
Acquisition Phase	Development, Acquisition
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1687

Statement:	Follow Active Directory naming conventions defined in "Active Directory User Object Attributes Specification," as required by the DoD CIO memorandum, "Microsoft Active Directory (AD) Services."
Rationale:	
Derived From	
Justifies	
Referenced By	Directory Services
Acquisition Phase	Development, Acquisition
Evaluation Criteria:	**1. Test:**

	Procedure: **Examples:**

BP1688

Statement:	For Services Management, use an interim solution of instrumentation of services and external monitoring.
Rationale:	This interim solution provides potential service consumers with real world historical performance metrics as well ensures that negotiated SLAs are supported.
Derived From	
Justifies	
Referenced By	Services Management
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1689

Statement:	Use the Service Discovery (SD) pilot program to practice and exercise the mechanics of service discovery and late binding.
Rationale:	The pilot program should be used to practice and exercise the mechanics of Service Discovery (SD) and late binding.
Derived From	
Justifies	
Referenced By	Service Discovery
Acquisition Phase	Development, Oversight

Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1690

Statement:	Use Node implemented Service Discovery (SD) for high availability.
Rationale:	One of the main reasons to develop a local Node Service Discovery (SD) Service is to support high availability.
Derived From	
Justifies	
Referenced By	Service Discovery
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1691

Statement:	Use Node implemented Service Discovery (SD) to meet compartmentalization needs.
Rationale:	For pilot implementations that are not reachable, such as might be the case in a higher classified environment, the Nodes should coordinate among themselves and DISA to provide pilot and full service implementations that are reachable.
Derived From	
Justifies	
Referenced By	Cross-Domain Interoperation, Service Discovery
Acquisition	Development, Oversight

Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1692

Statement:	The schedule indicates that progress on fielding the Collaboration Service should be monitored closely in the near term; take steps to determine actively which vendor offering to employ (perhaps hosting at the Node) if in a disadvantaged environment or separate network.
Rationale:	
Derived From	
Justifies	
Referenced By	Collaboration Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1693

Statement:	Make sure that collaboration products used to satisfy urgent requirements are from the JTIC list (see http://jitc.fhu.disa.mil/washops/jtcd/dcts/dctsv2 _software_list.html and, for products certified for use on SIPRNET, http://jitc.fhu.disa.mil/washops/jtcd/dcts/projects.html), until the Net-Centric Enterprise Services (NCES) Collaboration Service is available.
Rationale:	
Derived From	

Justifies	
Referenced By	Collaboration Services
Acquisition Phase	Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1694

Statement:	Coordinate with other Nodes having the same compartmentalization needs and with DISA to host compartmentalization CES.
Rationale:	The CES services will be provisioned by DISA and operated on the Non-secure Internet Protocol Router Network (NIPRNET) and Secret Internet Protocol Router Network (SIPRNET) global networks, initially operating from DISA Enterprise Computing Centers (DECCs). In order to have the CES to operate within a particular compartmentalization, a proactive role must be taken by the Node.
Derived From	
Justifies	
Referenced By	CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1695

Statement:	Designate a CES liaison to monitor the availability of services.
Rationale:	The CES liaison is an important role for keeping the Node and Component engineering processes synchronized with the Net-Centric

	Enterprise Services (NCES).
Derived From	
Justifies	
Referenced By	CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1696

Statement:	Use the Early Adopter process and service pilots to accelerate implementation of the CES services within the Node.
Rationale:	To accelerate the maturation and implementation of the CES, DISA established an Early Adopter process. Early adopters can participate in service pilots, as described in the Pilot Participant's Guide (draft). The Early Adopter process and service pilots should be used to accelerate implementation of the CES services within the Node. The decision to participate in the early adopter process and pilots is influenced by many factors, including acquisition phase, funding, mission, and priorities for individual systems as well as the aggregate Node.
Derived From	
Justifies	
Referenced By	CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1697

Statement:	Make the parallel development of CES outside the control of the Node a part of the Node's risk management activities.
Rationale:	Since the development of the CES is external to the development of the Node, there is an interdependency between the Node and the CES. The Node needs to consider this as an increase in the risk to the Node development. This risk needs to be communicated back to the CES management and development teams.
Derived From	
Justifies	
Referenced By	CES Parallel Development
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1698

Statement:	Do not expect cross-domain invocation of Component services within a Node.
Rationale:	Until such approaches are prototyped and explored more fully, Nodes should anticipate that services will not be capable of cross-domain invocation.
Derived From	
Justifies	
Referenced By	Cross-Domain Interoperation
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:**

	Procedure: **Examples:**

BP1699

Statement:	Configure routers in accordance with the Network STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1700

Statement:	Configure routers in accordance with Enclave STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Routers
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1701

Statement:	Configure Components for Information Assurance (IA) in accordance with the Network STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Network Information Assurance Components
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1702

Statement:	Do not place services and information intended to be broadly accessible to other nodes behind a VPN.
Rationale:	
Derived From	
Justifies	
Referenced By	Virtual Private Networks (VPN)
Acquisition Phase	Acquisition
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1704

Statement:	Consult the applicable Security Technical Implementation Guidance (STIG) documents as a fundamental part of design activities, and monitor the STIGs periodically for updates.
Rationale:	
Derived From	
Justifies	
Referenced By	Node Transport
Acquisition Phase	Acquisition, Development, Oversight
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1705

Statement:	Design DNS infrastructure in accordance with appropriate governing IPv6 Transition Office requirements.
Rationale:	
Derived From	**[**G1590**]**
Justifies	
Referenced By	IPv4 to IPv6 Transition, Domain Name System
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1706

Statement:	Anticipate that multicasting will be required even if not used currently and consider this requirement in the design of the Node's networks including the selection of Components and Configuration.
Rationale:	
Derived From	
Justifies	
Referenced By	Multicast
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1707

Statement:	Configure and locate elements of the Node Web infrastructure in accordance with the Web Server STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Infrastructure
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1708

Statement:	Configure and locate elements of the Node Web infrastructure in accordance with the Desktop Applications STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Infrastructure
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1709

Statement:	Configure and locate elements of the Node Web infrastructure in accordance with the Network STIG.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Infrastructure
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1710

Statement:	Support appropriate and widely accepted standards for Web portals provided by the Node.
Rationale:	
Derived From	
Justifies	
Referenced By	Web Portal
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1711

Statement:	Use the CES Mediation Service, or a locally hosted copy, when XML document translation between schemas is a necessity.
Rationale:	
Derived From	
Justifies	
Referenced By	Mediation Services
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**

BP1712

Statement:	Register developed mappings in the DoD Metadata Registry.
Rationale:	
Derived From	
Justifies	
Referenced By	Mediation Services
Acquisition Phase	
Evaluation Criteria:	**1. Test:** **Procedure:** **Examples:**